FEDERAL COMPUTER SECURITY MARKET

1990 - 1995

INPUT

About INPUT

INPUT provides planning information, analysis, and recommendations for the information technology industries. Through market research, technology forecasting, and competitive analysis, INPUT supports client management in making informed decisions.

Subscription services, proprietary research/consulting, merger/acquisition assistance, and multiclient studies are provided to users and vendors of information systems and services. INPUT specializes in the software and services industry which includes software products, systems operations, processing services, network services, systems integration, professional services, turnkey systems, and customer services. Particular areas of expertise include CASE analysis, information systems planning, and outsourcing.

Many of INPUT's professional staff members have more than 20 years' experience in their areas of specialization. Most have held senior management positions in operations, marketing, or planning. This expertise enables INPUT to supply practical solutions to complex business problems.

Formed as a privately held corporation in 1974, INPUT has become a leading international research and consulting firm. Clients include more than 100 of the world's largest and most technically advanced companies.

INPUT OFFICES

North America

San Francisco
1280 Villa Street
Mountain View, CA 94041-1194
Tel. (415) 961-3300 Fax (415) 961-3966

New York
Atrium at Glenpointe
400 Frank W. Burr Blvd.
Teaneck, NJ 07666
Tel. (201) 801-0050 Fax (201) 801-0441

Washington, D.C.
INPUT, INC.
1953 Gallows Road, Suite 560
Vienna, VA 22182
Tel. (703) 847-6870 Fax (703) 847-6872

International

London
INPUT LTD.
Piccadilly House
33/37 Regent Street
London SW1Y 4NF, England
Tel. (071) 493-9335 Fax (071) 629-0179

Paris
INPUT SARL
24, avenue du Recteur Poincaré
75016 Paris, France
Tel. (33-1) 46 47 65 65 Fax (33-1) 46 47 69 50

Frankfurt
INPUT LTD.
Sudetenstrasse 9
D-6306 Langgöns-Niederkleen, Germany
Tel. (0) 6447-7229 Fax (0) 6447-7327

Tokyo
INPUT KK
Saida Building, 4-6
Kanda Sakuma-cho, Chiyoda-ku
Tokyo 101, Japan
Tel. (03) 3864-0531 Fax (03) 3864-4114

AUGUST 1990

FEDERAL COMPUTER SECURITY MARKET

1990-1995

INPUT®

1953 Gallows Road, Suite 560, Vienna, VA 22182 (703) 847-6870

Published by
INPUT
1280 Villa Street
Mountain View, CA 94041-1194
U.S.A.

Federal Information Systems and Service Program (FISSP)

Federal Computer Security Market, 1990-1995

FISEC • 416 • 1990

Abstract

INPUT expects the federal government market demand for computer security products and services (excluding network security) to grow from $560 million in FY 1990 to $690 million in FY 1995. This represents a compound annual growth rate (CAGR) of 4%. The federal market for network security will remain constant over the next few years at nearly $400 million. These estimates exclude classified processing, since that data cannot be captured.

Federal Computer Security Market, 1990 - 1995 covers the forces, both positive and negative, driving this market. It also identifies what agencies will buy, how much will be bought, how it will be bought, and who will do the buying. The report compares agency and vendor perceptions of the market, and suggests some steps for vendors to take in expanding their market.

Table of Contents

Table of Contents (Continued)

Table of Contents (Continued)

Table of Contents (Continued)

Exhibits

Exhibits (Continued)

IV

V

Exhibits (Continued)

I

Introduction

The *Federal Computer Security Market, 1990-1995* is a new report concerning the market for security of federal information systems containing sensitive (but typically unclassified) information. The report was prepared in response to client interest in this emerging market and it identifies market issues and trends that impact current federal contractors and vendors entering or already in the security market through FY 1995. Insight into agency requirements, regulations, and contractor perceptions are offered to help vendors plan their strategies to compete for federal security contracts.

This report on security products and services applicable to the federal government was prepared as part of INPUT's Federal Information Systems and Services Program (FISSP). Reports issued through this program are designed to assist INPUT's U.S. industrial clients in planning how to satisfy future federal government needs for computer-based information systems and services. The report's findings are based on research and analyses of several sources, including:

- INPUT's Procurement Analysis Reports (PARs)
- OMB/GSA/NBS Five-Year Information Technology Plans for 1989-1994
- Interviews with leading vendors pursuing the federal computer security market
- Interviews with agency representatives
- Federal agency GFY 1989 and GFY 1990 Information Technology Plans
- Federal reports, studies, and other secondary research sources

A

Scope

The forecast period covered in the report is GFY 1990 through 1995. The surveys were conducted in 1989. Vendors were selected for interview because they were either identified as contractors already providing security-related products to the federal government or actively pursuing

this federal market. The agencies selected for survey are planning and implementing security for their systems which contain sensitive data.

For the purposes of this 1990 study, INPUT's definition of computer security encompasses the following categories of vendor products and services:

- Equipment
- Software Products
- Professional Services

This report supplements INPUT's previous reports on professional services. It is intended to give INPUT's clients a clearer understanding of the current status and future trends of the federal market for computer security. It also identifies the key vendors in the market, a subject of continuing interest to INPUT clients.

B
Methodology

In developing this report, INPUT used a variety of sources and methods. First, INPUT researched agency long-range plans and budget submissions for GFY 1990-1995 for major programs and new initiatives involving security of sensitive systems. Based on this research, INPUT pinpointed agencies and programs that related to computer security.

INPUT also reviewed its Procurement Analysis Reports (PARs) to develop further insight on agency activities. Many PARs cover programs that, for one reason or another, do not appear in the agency budget submissions. The PARs yield additional possibilities for further research.

Separate questionnaires were developed for agency officials and vendor respondents (see Appendix F).

- The agency questionnaire was designed to acquire information about current compliance with the Computer Security Act and plans for future implementation of security requirements.

- The vendor questionnaire was designed to acquire information on industry status and future federal market plans.

The same or similar questions were asked of both groups of respondents for comparative analysis. Federal agency officials selected for interview included:

- Agency executives at the policy level
- Functional program managers

The budgets, PARs, surveys, and secondary research were considered in developing the overall forecast.

Industry representatives selected for interview in the current and previous editions of this report included:

- Marketing executives
- Corporate executives
- Project/Program managers

The current versions of the Federal Information Resource Management Regulations, Federal Acquisition Regulations, Defense Acquisition Regulation (changes to FAR), and relevant federal legislation and agency regulations were investigated to identify provisions that will impact computer security contracts and/or contract performance.

C Report Organization

In addition to the introduction and appendixes, this report consists of five chapters:

- Chapter II contains an executive overview describing the major points and findings in the report.
- Chapter III provides the market forecast and describes the major market issues and trends impacting the industry.
- Chapter IV summarizes the federal agencies' requirements for computer security and the existing and planned implementation of security requirements.
- Chapter V presents vendors' perspectives on the federal computer security market.
- Chapter VI provides a sample of business opportunities for programs and initiatives in the federal market involving computer security.

Several appendixes are also provided:

- Interview Profiles
- Definitions
- Glossary of Acronyms
- Policies, Regulations, and Standards
- Related INPUT Reports
- Questionnaires

Following the appendixes is a description of INPUT and its programs and services.

II

Executive Overview

A Federal Market Pressures

The federal market for computer security products and services is expected to grow over the next five years. Exhibit II-1 lists some of the forces driving this growth, both in positive and negative terms.

EXHIBIT II-1

Federal Market Pressures

- Legislative mandate
- More information sharing
- Greater agency awareness
- Publicized network penetration
- Dedicated staffs
- Budget constraints
- Competing priorities
- Limited actual harm
- No follow-up legislation
- Poor planning effort

The Computer Security Act of 1987 (signed into law in early 1988) leads the list. It requires each agency to develop a computer security plan and initiate computer security training. Congress continues to encourage greater computer security. Most agencies have moved computing power to the end user and have enhanced information sharing through local- and wide-area networks, increasingly widespread use of microcomputers, and

relational data base approaches to managing agency information. This information sharing fosters compatibility and interoperability standards, leading to demands for a more open network architecture. However, the security risk increases as it becomes easier to share information over open networks.

Further, many agency executives have become increasingly aware of the need for computer security. A variety of factors are driving this increased awareness. The penetration of the DoD's Internet network, which was heavily covered by the media, probably did more than anything else to increase security awareness. NIST, NSA, and other government agencies have established dedicated staffs to protect computer systems. Some momentum currently appears to be growing for greater privacy. All these forces are driving the need for improved computer security in federal agencies.

On the other hand, there are also some market forces which discourage the growth of federal computer security. Continuing budget constraints are the biggest single inhibitor. Some of the oversight agencies have had their own computer security budgets cut, in part for irrelevant reasons. Individual agencies operating under constrained budgets are also trading off enhanced computer security for greater operational effectiveness. This is especially true in the Tempest equipment market, which is practically flat. Many agencies are allocating their limited resources to other, more pressing initiatives, whenever there appears to be a greater payoff.

Most agency executives and Congressional decision makers do not appreciate the potential loss from security mishaps. The Internet virus did little real harm, as has been the case with most security breaches. Until major damage occurs which might involve loss of life or major property loss, few significant market changes will occur.

Despite several attempts in 1988 and 1989, Congress failed to pass any follow-up computer security legislation. This showed a reduction in congressional concern, and with it a lessening in appropriation efforts. Although the development of agency security plans represented a positive factor, the quality of those plans has to be viewed as a negative. Among other things, these plans

- Overlooked integrity and availability requirements
- Failed to involve user organizations
- Omitted, for the most part, network security

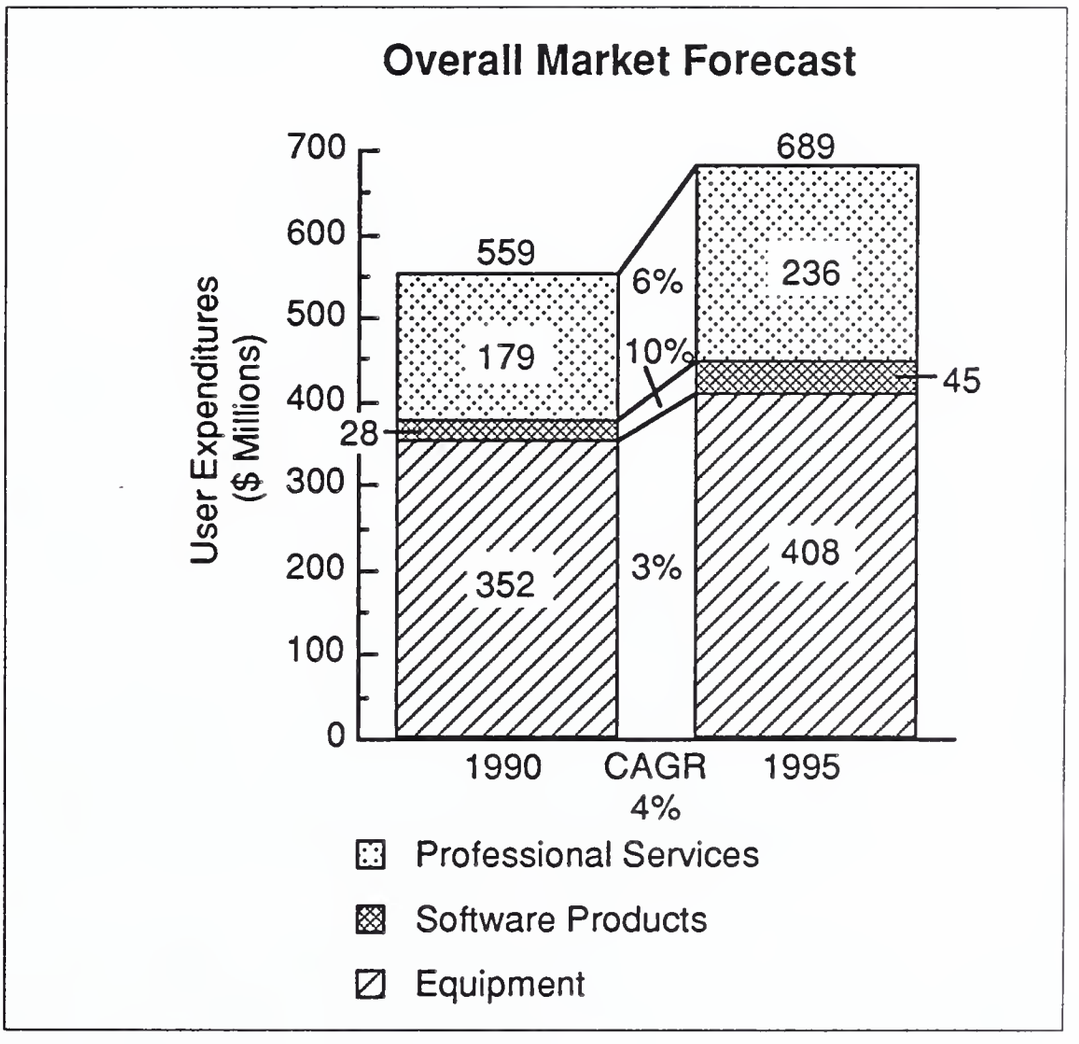
This suggests that, for many agencies, the planning effort became a mere paperwork exercise.

B

Market Forecast

INPUT expects that the federal computer security market will grow from $559 million in FY 1990 to $689 million FY 1994, at a compound annual growth rate (CAGR) of 4%. Exhibit II-2 displays a breakdown of this market into 3 subordinate areas.

EXHIBIT II-2



As noted in the exhibit, software products will show the fastest growth rate, as agencies use them to improve security in their installed systems. The equipment market will remain fairly flat at a CAGR of only 3%, reflecting

- Reduced demand for Tempest products
- A relaxation of some Tempest standards
- Growing cost-effectiveness of Tempest technology

Network security, consisting primarily of encryption equipment, is excluded from INPUT's forecast model because of the embedded nature of its processing. However, it still represents a major business opportunity in the federal market. INPUT has sized this market at $396 million annually, and expects it to remain fairly flat over the forecast period. Although demand is increasing, particularly among civilian agencies, the

growing cost-effectiveness of data encryption equipment is offsetting this growth, leading to the flat market projection.

C

Leading Vendors

INPUT encountered a fairly wide divergence of opinion on the identity of the leading vendors in the federal computer security market. Exhibit II-3 compares agency and vendor responses to this question.

EXHIBIT II-3

Views on Leading Computer Security Vendors

Agency Views	Vendor Views
Comsis	Digital Equipment
Honeywell	AT&T
IBM	IBM

Only IBM made the top 3 of both lists. Comsis is an 8(a) firm which won a GSA contract to help agencies develop their security plans. DoD agencies think of Honeywell in terms of the World Wide Military Command and Control System. It is interesting to note that Digital was rated first by the vendors, but was not mentioned by a single agency.

D

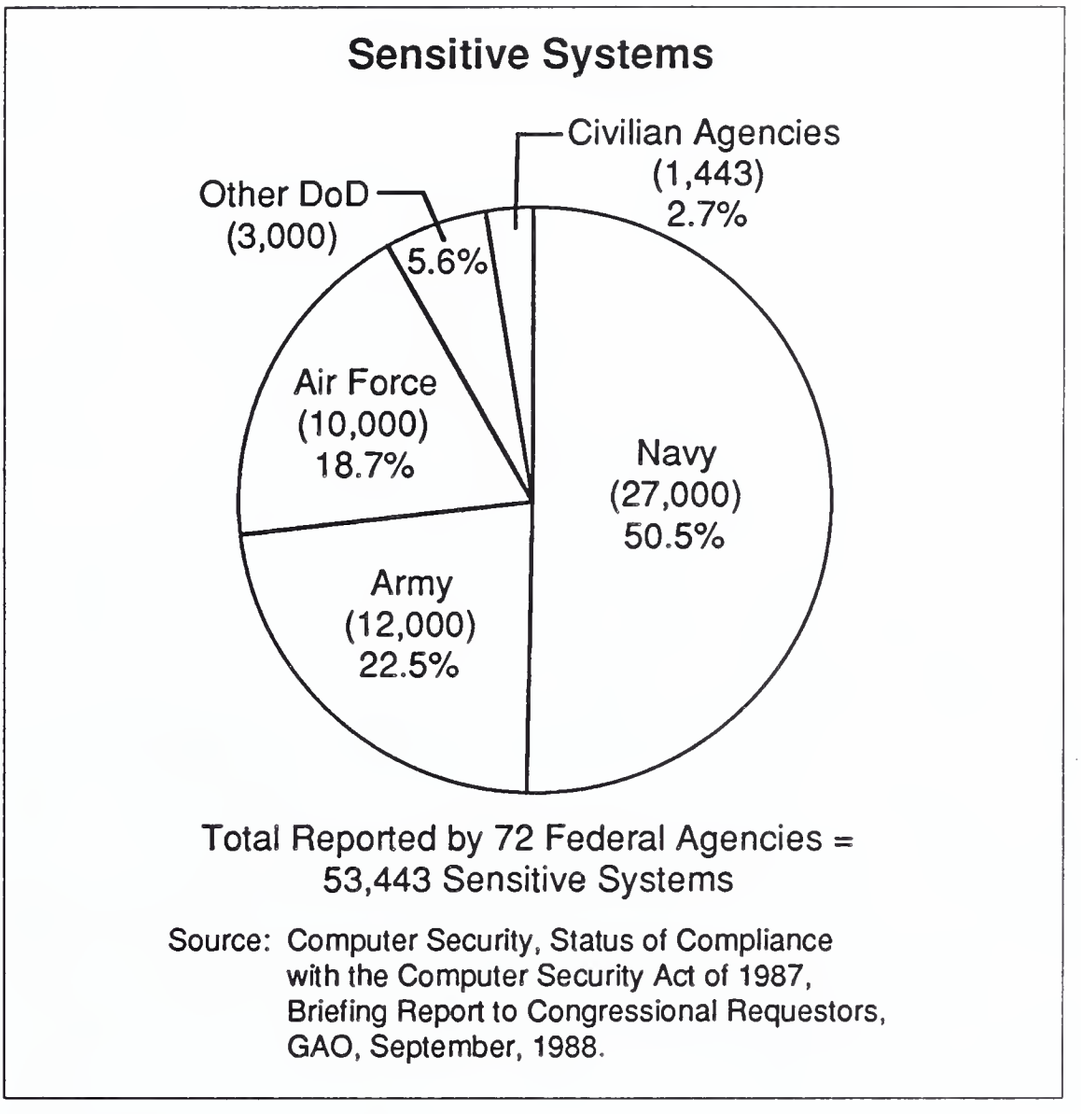
Sensitive System Population

In 1988, the GAO reported 53,443 sensitive systems itemized by 72 agencies responding to a survey. Exhibit II-4 summarizes the results to the survey. Two interesting findings emerge:

- More than 97% of all sensitive systems belonged to the Defense Department. This may actually overstate the proportion somewhat, due to reporting and definition- related irregularities. However, it is obvious that most of the target market is in Defense. However, when the vendors were asked which agencies offer the greatest opportunities, the Treasury Department headed the list.

- More than half of all sensitive systems were listed as in the Navy. This is surprising, given the volume of work in the other military services. It may reflect, however, reporting and definition irregularities. However, it certainly suggests that vendors with limited marketing resources should concentrate on the Navy.

EXHIBIT II-4



Further research shows that many civilian agencies aggregated their systems, thus reducing the total number. Defense agencies, however, did not consolidate systems, which drove up their numbers. This suggests that vendors may pursue far more than the 53,000 systems that the GAO identified.

E

Functional Requirements

Exhibit II-5 summarizes the results of the survey of functional requirements for computer security. Most agency respondents provided more than one answer. All participants in the agency survey specified the need for network security, although it is unusual for agency respondents to agree universally on anything. This response suggests the importance agencies assign to securing their networks. INPUT has found in other surveys that agencies rely heavily on their networks.

EXHIBIT II-5

Functional Requirements for Computer Security

Requirement	Percent of Respondents*
Network Security	100
End-User Access	95
Data Security	91
Physical Security	86

*Adds to more than 100% due to multiple responses.

The other functional requirements listed in Exhibit II-5 also received high ratings. In INPUT's view, these accurately reflect agency needs in computer security. Functional safeguards to assure limited and proper access to sensitive data include encryption techniques, passwords, and multilevel security operating systems. Data security helps agencies protect the accuracy, integrity, and continuity of stored information. Physical security, often the least costly requirement, includes access to computer centers, remote processing sites, and any additional LAN or WAN sites.

F Acquisition Methods

By a fairly sizable margin, most agency respondents stated that they prefer to use the GSA Schedule to acquire computer security products and services. Exhibit II-6 shows the results of this survey question. The schedules are most appropriate for software-related products and training tools, particularly less expensive items. However, some security-related services are available through GSA contracts, and respondents may have been including them with the schedules.

Solicitations for specific purchases and requirements contracts received almost equal ratings. There is a growing trend among agencies to use requirements contracts in a variety of areas, and this is apparently extending to computer security.

Security products are also being acquired as part of other procurements, such as Treasury's TMAC and DMAC procurements, which were cited by agency respondents. Further, most systems integration solicitations contain security requirements, included within other functional requirements.

EXHIBIT II-6

Methods of Acquisition

Method	Percent of Respondents*
GSA Schedules	85
RFP for Specific Purchase	60
RFP for Requirements Contract	55
Purchase Security Devices as Part of Other Procurements	40
Other Methods	20

*Adds to more than 100% due to multiple responses.

G

Recommendations

In providing computer security products and services to the federal government, vendors need to take a flexible approach. While there are clearly some definite needs, as in network security, likely spending remains somewhat ambiguous. If Congress continues to pressure the agencies, spending may increase slightly more than forecast, but probably not much.

Vendors need to align their products and services to meet agency expectations, and then market heavily. To some extent, vendors need to create a demand for their capabilities by demonstrating tangible benefits to the government customer. In this way they can secure a worthwhile share of this growing market.

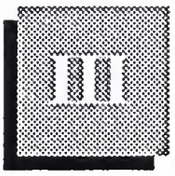
Much agency buying in computer security will come through systems integration contracts, which do not focus specifically on computer security. Therefore, those vendors specializing in computer security should establish teaming relationships which enable them to participate in large, complex bids.

Finally, security vendors should develop products which accommodate the widely varied systems and equipment types in the federal market. To the extent that security products accommodate applicable federal standards, potential market penetration will increase. Exhibit II-7 summarizes these recommendations.

EXHIBIT II-7

Recommendations

- Develop a flexible marketing approach
- Align products to agency expectations
- Create demand by demonstrating tangible benefits
- Establish effective teaming arrangements
- Develop portable and interoperable products



Market Analysis and Forecast

A
Market Evaluation and Development

Computer security for the federal government focuses on protecting the integrity of federal information systems. The concept of integrity in government information entails the confidentiality of data to which access should be limited, such as personal, proprietary, and national security classified data. It also includes assuring the accuracy and accessibility of information so that the public can be informed and agencies can discharge their duties efficiently and responsively.

In support of federal agency missions and applications, computer security assists with the management of systems in performing the appropriate functions. Security works to protect information in the systems from unauthorized disclosure and unauthorized or inadvertent modification. It also ensures that information is available on a timely basis. However, it is important to note that in many federal systems, such as weather monitoring systems, protection from disclosure is not the primary security needed since the information is intended for widespread dissemination.

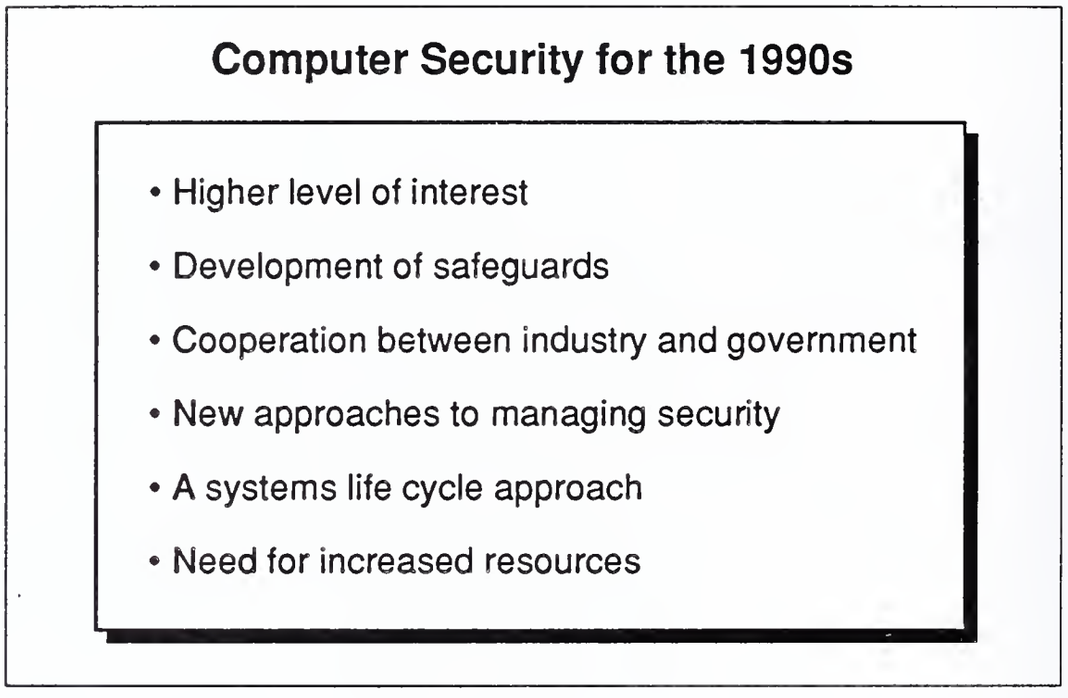
The government's management and regulation of the security of its information technology systems has a lengthy history of executive policies and legislative/regulatory initiatives. These are discussed in Section E.

Exhibit III-1 summarizes some key security issues:

- Compliance with the Computer Security Act will promote a higher level of interest in federal computer security issues.
- Incidents such as the Internet virus will foster the development of greater security safeguards.
- New research and technology requirements will necessitate cooperation between industry and government.

- Increased networking requires new approaches to managing security, especially as it relates to microcomputers.
- Agencies require a systems life cycle approach to security to coincide with their standard development process.
- Agencies need an increased allocation of resources for security, an unlikely development under present circumstances.

EXHIBIT III-1



Computer security places an additional strain on already tight agency budgets. Aware that retrofitting systems is excessively expensive, some agencies are adopting a systems life cycle approach to security. Government-wide, an increase in manpower and funding is needed for the implementation of security plans, federal employee training, and installation of security controls for government information systems.

Defense concerns about computer security led to the publication in 1983 of the *DoD Trusted Computer System Evaluation Criteria*, commonly referred to as the "Orange Book." DoD published a revised standard in 1985, with the same name and the code of DoD 5200.28-STD. The Orange Book established a series of computer security rankings, which are summarized in Exhibit III-2.

EXHIBIT III-2

Computer Security Levels

- Division A: verified protection
  - Class A1: verified design
  - Beyond Class A1: future technology
- Division B: mandatory protection
  - Class B1: labeled security protection
  - Class B2: structured protection
  - Class B3: security domains
- Division C: discretionary security protection
  - Class C1: discretionary security protection
  - Class C2: controlled access protection
- Division D: minimal protection

In evaluating federal computer security in the 1990s, vendors need to take a cautious approach to Orange Book standards. These standards may be at least partially supplanted. The European community is proceeding somewhat differently in establishing standards. A meeting is scheduled in Brussels in September, 1990, which may formally establish different standards, tied to the International Standards Organization.

This development would appeal to many vendors, who have long complained about the length of NSA review and NSA's refusal to follow anyone else's evaluation. Staffing patterns at NSA may also serve to reduce its influence in the federal market. Recently, NSA cut its computer security staff to fewer than 20 people, now reporting to officials working in NSA's traditional communications security area. These changes suggest that NSA will play a less dominant role in federal computer security.

Despite the passage of the Computer Security Act in late 1987, relatively few agencies showed much interest in computer security. This changed at least temporarily in November, 1988, when a virus penetrated thousands of computers on Internet, an unclassified multinetwork system connecting more than 60,000 computers nationally and internationally. The interest of the press, the public, and subsequently the Congress led to still another GAO report. Federal funding contributes about $50 million

annually to Internet, with most coming from the National Science Foundation (NSF) and DoD's Advanced Research Projects Agency (DARPA). GAO identified several Internet vulnerabilities:

- No Internet security focal point
- Security weaknesses at host sites
- Weak procedures for correcting software holes

At this writing, a college student has been convicted for his involvement in the virus. As might be expected, the Congress expressed concern over the developments, but did nothing. Section III.E. covers the legislative attempts of 1989.

Early in 1989, a team of security experts began reviewing the security plans required from each agency by the Computer Security Act. Personnel from the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) comprised the team. Initially, the civil agencies submitted 1,700 plans, while the defense agencies submitted only three plans. This apparently resulted from a misunderstanding on jurisdiction. Subsequently, in August 1989, Defense agencies submitted 29,000 plans. Although the team obviously could not review all these plans, it did provide 450 sets of comments. In general, the team identified the following problems with the plans:

- Integrity and availability requirements were overlooked.
- Confidentiality issues were overly stressed.
- User organizations apparently did not participate in the development of the plans.
- State and local government organizations with federal funding, as well as federally funded contractors, failed to provide any plans.
- Few plans addressed network security.
- Few plans covered microcomputers adequately.

Despite these problems, NIST cited some benefits to the overall process:

- Many federal agencies performed security planning for the first time.
- Other agencies reevaluated their security planning practices.
- Most of the review team's comments were well-received by the agencies.
- Despite fears to the contrary, NIST and NSA worked well together on the review effort.

In May, 1990, GAO published a brief report on the security planning process. As might be expected, GAO had little positive to say:

- The security plans had limited impact on agency computer security programs.
- The plans lacked adequate information to serve as effective management tools.
- Managers had insufficient time to prepare the plans.
- Guidance was sometimes unclear and misinterpreted by agencies.
- Agencies have not implemented most planned security controls.
- NIST/NSA review and feedback was general and of limited use to agencies.

GAO did add that new OMB guidance on security planning may assist future agency planning efforts. However, the results suggest that vendors need to develop a strong marketing effort, in order to create greater demand among the agencies.

B

Market Structure

The federal computer security market, like many other specialized areas, may be broken out into various distinct segments, as follows:

- Computer security equipment includes both processors and peripheral equipment which are Tempest-shielded (i.e., electronic or electromechanical emanations are blocked), as well as processor-based equipment used in the protection of computer systems. For the purposes of this report, this category does not include electronic locking systems, fire protection systems, or encryption devices. General purpose computer systems which have been modified are included, as well as Tempest-protected CD ROM products, such as those from Memory Storage Devices. This category does not include electronic access control devices, such as the Retinal Scan device from Eye Dentify, Inc.
- Computer security software products include any commercially available product whose primary function is to enhance the security system. It does not include general purpose operating systems which incorporate standard security features. However, software specifically aimed at security is included. For example, the Sun OS MLS, a multilevel secure UNIX operating system, is included, as are the various antivirus products, such as N-Vir Assassin for the Macintosh or Vi-Spy for the IBM PS/2. Software products supporting communications security, such as Verdix's VIbus interface and 3COM's upgraded security features on its network control servers, are also included, as are mainframe products such as IBM's RACF and CA's ACF II.

- Professional services includes INPUT's four delivery submodes:

- Consulting services includes feasibility studies, requirements analyses, risk analyses, security plans, and system audits. Many agencies used consultants to assist them in writing the new plans required by the Computer Security Act. However, this appears to have been a one-time opportunity, since NIST is not expected to require updates.

- Education and training is an important component of this market, since the Act requires that all federal employees with access to computer files receive training. There are several companies currently supplying computer security training. Further, the Office of Personnel Management, with contractual help from Advanced Technology, Inc., is providing training to federal employees.

- Software development relates to custom-tailored efforts to enhance security at a particular client, location, or system. Modifications to standard products to suit a particular client's security needs also fall into this category.

- Systems operations relates to those operational activities specifically aimed at enhancing computer security.

The federal computer security market includes other products and services that operate in classified environments. For example, Unisys' Blacker system, supporting network security, is currently being evaluated for A1 security rating by the National Computer Security Center (NCSC) at NSA. Similarly, the Xerox Encryption Unit is also being evaluated by NCSC. Software to facilitate NSA code breaking might also be considered a computing security product.

Information on acquiring these products is classified, making it impossible to develop market sizing information. Accordingly, INPUT has not included them in this market structure or in the market forecast provided in the next section. However, when general information on these products and services is publicly available, INPUT has included that information in this report.

Perceived Market Differences

Agency and industry respondents were asked their opinions on the differences between the defense and civilian agency markets for computer security products and services. Exhibit III-3 compares the agency and vendor perceptions obtained. In general, the responses present different perspectives—the agencies as users and the vendors as suppliers.

EXHIBIT III-3

Perceived Differences— Civilian and Defense Markets

Agency Respondents	Rank*	Industry Respondents
Market Increasing More Rapidly in Civilian Sector.	1	Defense Market Subject to Stricter Standards and Requirements.
More Defense-Oriented Products Available.	2	Employees at Civilian Agencies Have Less Security Training and Awareness.
Defense Agencies and State Department Most Active in Establishing Security Requirements.	3	Differences in Volume of Classified Data (DoD Greater)
Banking and Insurance Industry Security Will Impact Civilian Agencies—Especially Treasury Department.	4	Increased Opportunities for Custom Solutions in Defense Agencies.

*Rank based on frequency of mention by respondents.

The agency respondents directed some of their comments to the more rapid growth in the civilian market. In their opinion, the civilian market is also subjected to stronger influence from the commercial industries. Several respondents pointed to the Treasury Department as a prime example. They expect computer security to be emphasized more at civilian agencies that address financial and law enforcement matters. Less emphasis is expected at agencies with scientific missions, since they require shared technical information to be widely accessible.

From the vendors' perspective, the defense agencies appear to be more likely potential targets for their products and services, since many vendors are already well-known at some agencies and are more familiar with the agencies' information systems. The civilian agencies are viewed as a growing market for products, due to the additional security requirements the agencies have added to comply with government legislation. Further, some security agencies also manage classified information.

The majority of industry respondents noted that there are more numerous and stricter requirements and standards imposed upon the defense agencies which are not applicable to the civilian agencies. These requirements and standards in turn increase vendor opportunities to provide customized hardware and software for computer security installations.

Another notable difference from the vendors' point of view was the greater level of awareness and training at defense agencies. At the civilian agencies there is a greater need for training to bring employees up to the level of awareness required by the Computer Security Act. This training is already underway at most agencies.

C Market Forecast

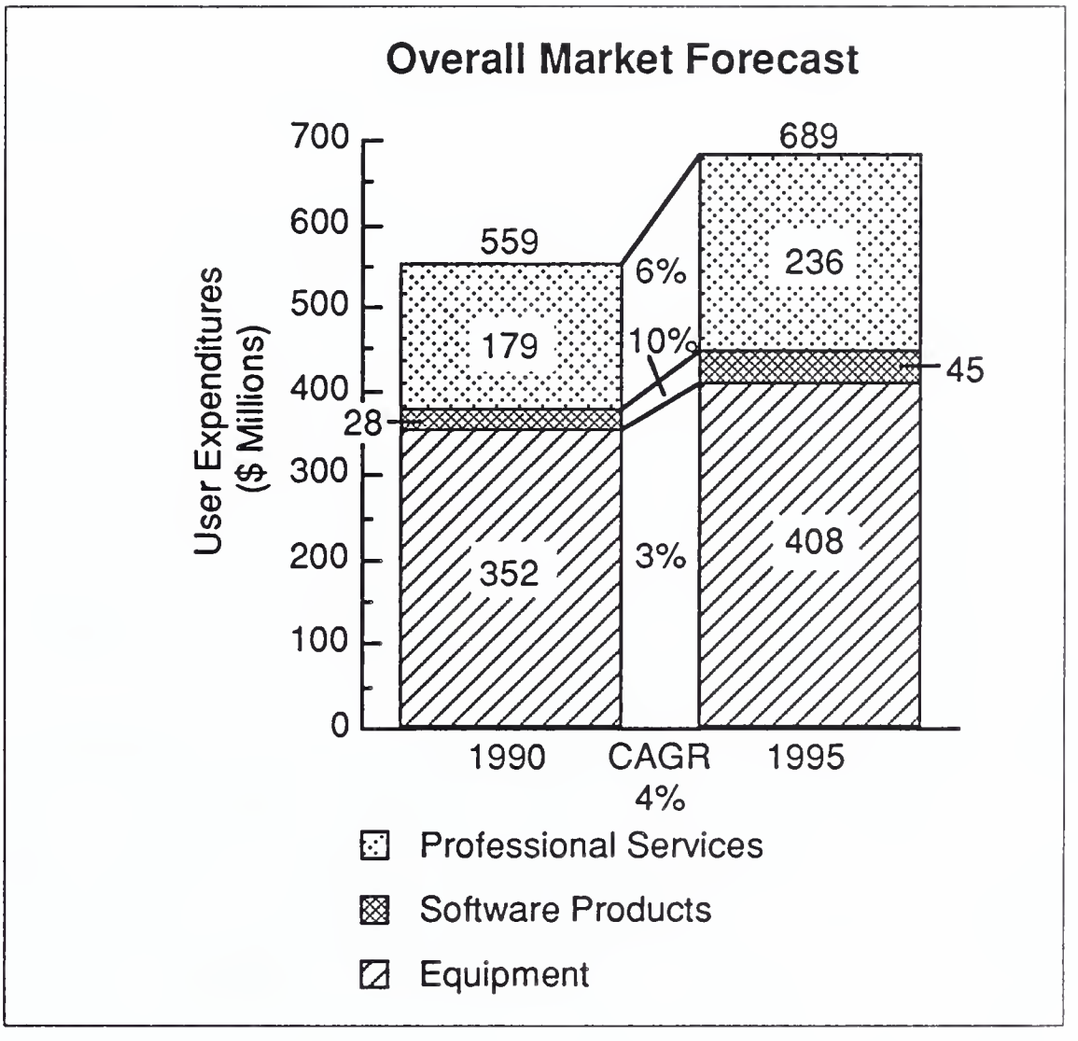
The federal computer security market will grow from $559 million in FY 1990 to $689 million in FY 1995, at a CAGR of 4%, as shown in Exhibit III-4. With inflation factors taken into account, this could be considered a declining market. As described in the previous section, this market includes the equipment, software products, and professional services that operate in an unclassified environment. With classified applications added, the market size would probably increase sharply. However, since such information is not publicly available, it is omitted from this forecast.

In part, the overall federal IS market is determining the viability of the federal computer security market. The extent to which agency program managers include security requirements in their solicitations will drive both market size and complexity. The Computer Security Act defined sensitive information as that whose "loss, misuse, or unauthorized access to or modification...could adversely affect the national interest or the conduct of federal programs or the privacy to which individuals are entitled under [The Privacy Act]."

Therefore, solicitations that place a high premium on confidentiality, integrity, and availability will spur the need for products and services. The Computer Security Act also requires annual security reviews. If OMB enforces this requirement, it will lead to significant opportunities for professional services firms. On the other hand, if these reviews become a paperwork exercise, most agencies will apply few resources to the effort.

Although computer viruses receive much media attention, NIST has stated that they are not the major problem. Rather, NIST stresses the need for security management and oversight. If this view spreads throughout the government, professional services opportunities might grow at the expense of software products. This counters the overall federal IS trend, which currently favors software products over professional services.

EXHIBIT III-4



In defining the federal computer security market, it is helpful to examine market issues among various market segments:

- Processing Services: Computer security takes several forms in contractor-operated agency processing environments, both government-owned and contractor-owned. Two NASA COCO facilities, at Goddard Space Flight Center and Ames Research Center, have established Computer Security Incident Response teams. The FBI has established a Library Awareness Program to monitor circulation, on-line data base, and inter- and intralibrary programs, to ensure data integrity.

- Professional Services: The federal government will spend ample sums on professional services support to help meet its computer security needs. First, as already pointed out, the Computer Security Act requires appropriate training of appropriate personnel. Although OPM has become very active in this area, various private providers are also providing computer security training to federal personnel. Consulting support will continue to be needed for security evaluations and audits, as well as for upgrading computer security measures. However, if the agencies are not required to submit updated security plans, the volume

of planning opportunities will likely disappear. Custom software development will also play an important role. For example, IRS hopes to achieve C2-level security for its Tax System Modernization program. Unique software development will be needed to achieve that goal.

- Software Products: The growing availability and functionality of software products, especially in the area of network security, is spurring this market. For example, it has been reported that the market for secure UNIX products has grown sharply as a result of the Internet virus. The Small Business Administration is using software products to define its computer security needs. SBA developed its "BASIC" software procedures in conjunction with the Federal Judiciary Center and the Department of Veterans Affairs. Despite the fact that the software itself does not actually protect anything, it still needs to be included in the software products segment of the federal computer security market, since its usefulness and salability depends on that market.

- Computer Equipment: As indicated in the previous section, specialized computer equipment, including Tempest-shielded equipment, forms the primary (in terms of funding) component of the federal computer security market. Much of this equipment is listed on the Preferred Products List (PPL) developed and maintained by NSA. However, the PPL has been criticized as being too lax in enforcement of its standards. In response, NSA is moving toward more exacting standards with its Endorsed Tempest Products List (ETPL). An even more exacting list, the Potential ETPL, is also under consideration. These lists, plus some relaxation in Tempest standards, have led to some market confusion. The DoD budget cuts are aggravating this problem.

- Telecommunications: The network security market was discussed briefly in the preceding section. Although from a technical standpoint LANs may not involve telecommunications, INPUT includes them in the telecommunications category because of the similar functions. LAN use in the federal market has grown considerably. As a result, NIST is seeking password generators from the vendor community. Presumably, NIST will foster sales opportunities for these products, once they become available, through interagency conferences and general publications.

- Electronic Data Interchange (EDI): As reported in INPUT's *Federal EDI Market* report, budget constraints are encouraging greater use of EDI in the federal market. As EDI becomes more commonplace, the potential for security violations increases, which concerns both agencies and vendors. In the agency and vendor surveys for this report, INPUT asked about the impact of security requirements on EDI and

CALS. Exhibits III-5 through III-8 summarize the results. It should be noted that most of the responses for EDI also applied to CALS. These responses suggest some limited concern on the part of agencies and vendors.

EXHIBIT III-5

Agency Views of Security Regulations' Effect on EDI Initiatives

- Delay of approved classification
- Privacy/data integrity requirements
- Additional complexity of initiatives
- Additional security required of software
- None

EXHIBIT III-6

Vendor Views of Security Regulations' Effect on EDI Initiatives

- Increased costs
- Need to integrate with other systems
- Need for improved NIST standards
- Regulations not yet solving EDI security problems

EXHIBIT III-7

Agency Views of Security Regulations' Effect on CALS Initiatives

- Increased software security capabilities
- Insufficient guidance on CALS standards
- Delay of approved classification
- Additional complexity of initiatives
- None

EXHIBIT III-8

Vendor Views of Security Regulations' Effect on CALS Initiatives

- Increased costs
- Need to integrate with other systems
- Risky concentration of sensitive data
- Additional restrictions being imposed
- Need to insure data integrity
- Need to increase priority of CALS security

One other market issue which might affect vendor sales prospects is the on-again, off-again dispute between NIST and NSA. The problem originally surfaced with the passage of the Computer Security Act, which gave broad powers to NIST, some of which formerly belonged to NSA. The dispute nearly disappeared in 1989, when the two agencies apparently worked very effectively together in reviewing agency security plans. However, by early 1990, problems resurfaced as Congressional pressure increased.

In particular, the House Government Operations Committee may force changes to the memorandum of understanding between the two agencies. The committee wants to insure that NIST plays the primary role in computer security policy in the civilian agencies. To complicate matters further, National Security Directive Document 145, despite two revisions, still appears to conflict with the Computer Security Act.

These disputes are complicating sales efforts for many vendors and agencies. It is sometimes difficult for vendors to determine who is in charge. The agencies are having the same problem. INPUT expects new legislation to be enacted in 1990 which will resolve the dispute.

INPUT's market forecast is lower than other estimates reported in the press. For example, another market analyst estimated that procurement of Tempest equipment, with added secure telephones, could rise to more than $1 billion by 1994. Apparently, this forecast is based primarily on past sales patterns, relaxation in some agency Tempest requirements, and growing recognition of the importance of Tempest products in various categories.

Unfortunately, the Defense IRM budget cuts of nearly $600 million in FY 1990 included initiatives requiring Tempest-approved computers and equipment. Though cuts were widely anticipated, the magnitude exceeded most forecasts. These cuts have tended to reduce demands for Tempest equipment. Instead of automatically including Tempest requirements, many agency program managers, facing budget constraints, are questioning the need for Tempest shielding and seeking ways to avoid it.

The growing cost-effectiveness of Tempest technology is also dampening market growth. An analysis of the history of Tempest-approved computer prices shows that most systems now cost only 50%-75% more than comparable non-shielded systems. As a result, when protection is required, agencies can often obtain it more economically than was possible several years ago.

Similarly, spending on software products and professional services will be fairly constrained, although the former will grow at a healthy 10% rate. However, if an expensive or life-threatening security violation should occur, the situation could change drastically. Congress would be expected to recognize the problem and fund accordingly.

Network security also represents a significant business opportunity in the federal market. Strictly speaking, this market is outside INPUT's model, since it consists of data encryption and other equipment usually excluded from INPUT's categories. However, numerous software products, such as the software controls on 3COM's network servers and Verdix's VIbus interface, are included in INPUT's software products forecast.

INPUT estimates that the current federal market for network security products and services is $396 million, and it is expected to remain flat over the next few years. However, INPUT expects the civilian share to increase with corresponding cuts in Defense. The press has reported market estimates ranging from $341 million to more than $2 billion. INPUT's estimate falls on the low side of that range, based on current and expected future Defense budget cuts. The growing cost-effectiveness of data encryption equipment is also expected to keep this market relatively flat.

This market could increase, however, if the vulnerability of public switched network systems increases. There have been rumors of AT&T losing control of central switches, and the Secret Service looking into this. If this is true, it may presage a new federal initiative on enhanced security of public communications systems.

D

Federal Market Pressures

There are competing market pressures driving this market. Exhibit III-9 lists the major pressures. On the positive side, the Computer Security Act of 1987 (signed in early 1988) required that each agency develop a computer security plan. However, the requirement for computer security training probably did more to encourage greater understanding and appreciation of the problem among federal officials.

EXHIBIT III-9

Federal Computer Security Market Pressures

- Encouraging computer security expenditures
  - Legislative mandate
  - Greater end-user computing
  - More information sharing
  - Open network architecture
  - Greater agency awareness
  - Publicized network penetration
  - Dedicated staffs
- Discouraging computer security expenditures
  - Budget constraints
  - Competing priorities
  - Limited actual harm
  - No follow-up legislation
  - Poor planning effort

As in the private sector, most federal agencies have moved computing power to end users through microcomputers, workstations, and local-area networks (LANs). Many agencies require greater sharing of information, which fosters compatibility and interoperability standards. This leads to requirements for greater ease of use. Agencies put a premium on software features which reduce human effort and error. However, these same features tend to enhance the risk of security violations. The systems' ease of use encourages ease of abuse. The open network architecture which many agencies require often includes the mandatory use of

the Government Open System Interconnect Profile (GOSIP) standard. All of these information sharing initiatives represent a threat to computer security and safety.

The Internet virus in late 1988 served to heighten agencies' awareness of their vulnerabilities. The virus apparently entered the network's UNIX operating system through a hole in the electronic mail system. It then shut down other operations and sent copies of itself to other computers on the network. It appears that no lasting harm was done. Lasting harm may have actually spurred the federal computer security market to higher funding levels. At any rate, the incident received (and continues to receive) great notoriety in the media, thus increasing an appreciation of the importance of computer security.

Finally, on the positive side, both the NIST and the NSA have staffs dedicated to computer security. To the surprise of some federal pundits, these staffs worked well together in reviewing the agency plans. NIST personnel, in particular, frequently speak of agency and commercial conferences on the importance of computer security in the federal government.

As indicated in Exhibit III-9, there are also some market pressures which discourage growth of the federal computer security market. Budget constraints, by far, account for the strongest restraint. NIST had been expecting to receive $6 million in FY 1990 funds for computer security. However, this figure was cut to $2.5 million, the same amount appropriated in FY 1989. Press reports indicated that the cut was directed by an Iowa Congressman who was in a dispute with the NIST on an unrelated matter. Thus, as so often happens in the federal market, funding decisions hinge on extraneous issues.

On a more global level, many agencies, especially defense agencies, are currently suffering budgetary shortfalls. Individual programs are being cut and, in some cases, employees are being laid off. In the absence of tangible evidence to the contrary, it is difficult to see an immediate payoff to computer security. In most agencies, computer security spending is being reduced to permit emphasis of higher-priority projects.

As pointed out above, the Internet virus did little real harm. This has generally been the case with most security breaches. Until apparent major damage occurs, few significant changes will occur. To consider a worst case scenario: Suppose a virus entered the FAA's Air Traffic Control System, precipitating a mid-air collision. If such a horrible event occurred, Congress would likely move quickly to improve federal computer security. Irrelevant disputes with an Iowa Congressman would no longer matter. However, until some really serious crisis occurs, politics as usual will likely control federal computer security. The failed attempts at follow-up legislation, discussed in detail in section III.E., show the lack of any Congressional sense of urgency.

Although the development of agency security plans represented a positive factor, the quality of those plans has to be viewed as negative. Some of these weaknesses were discussed in Section III.A. Since NIST does not intend to require a second submission, many agencies will not have usable plans, at least for the foreseeable future.

E

Laws, Regulations and Policies

The federal government has taken a series of steps to enhance computer security:

1978 - Issuance of Transmittal Memorandum to OMB Circular No. A-71 (which was effective March, 1965). The memo promulgates policy and responsibilities for the development and implementation of computer security programs by executive branch departments and agencies.

1985 - Issuance of OMB Circular No A-130. The circular contains the OMB guidance relevant to security in the development of automated information systems. A-130 is an omnibus circular intended to summarize OMB guidance across all aspects of information systems. It rescinds OMB Circular No. A-71.

1988 - Computer Security Act of 1987, signed into law in January 1988. (P.L. 100-235). The Act calls for development security standards, establishing security plans, and implementing a comprehensive training and awareness program for all employees involved with federal computer systems containing sensitive information.

1989 - OMB issued guidance for preparation of security plans for computer systems containing sensitive information in order to assist agencies in preparing their computer security plans.

1990s - Administrative and policy formulating agencies (NIST, GSA, NSA, OMB) will develop further guidance for assuring that computer security planning decisions are integrated with basic budgetary decisions for information technology systems.

Additionally, the General Accounting Office (GAO) issued more than 40 reports between 1976 and 1988 on computer security. Most of these reports criticized agencies for operating systems which are highly vulnerable to both internal and external threats. The GAO reports cited both personnel and systemic problems which lead to breaches in agency security.

These reports were supplemented in the early 1980s by additional studies performed by:

- The American Institute of Certified Public Accountants
- The American Bar Association
- The President's Council on Integrity and Efficiency (which reviewed ten federal centers)

These studies increased agency awareness and understanding of the growing security problem. Subsequent testimony in 1985 by GAO and other officials further highlighted the federal security problem and helped lead to new security legislation. Unfortunately, none of the reports told agencies how to secure the necessary resources to improve their computer security.

The growth of end-user computing in the federal market serves to aggravate the computer security problem. The microcomputer has drastically altered the way information is created, stored, and used. The networks which tie these microcomputers together increase the opportunities for computer hackers to penetrate restricted systems. The networks also increase the risk of computer viruses disrupting government systems. While these networks are often indispensable to the conduct of government business, they also increase the government's vulnerability.

Following the Watergate scandals of the early 1970s, Congress mandated a physical break in the transmission of personal tax information. Thus IRS was inhibited in its networking efforts. Even today, IRS mails magnetic tapes containing taxpayer information between the ten service centers and the National Computer Center in Martinburg, West Virginia.

Congress has the difficult task of enacting laws to combat computer security violations but yet not restrict access to data that should be distributed and shared among federal system users. It also faces the challenge of keeping a balance among the various federal agencies which promulgate regulations, standards, and protect the national security. Legislators, in their enactment of the Computer Security Act of 1987 (P.L. 100-235), finally succeeded in reaching a compromise regarding the roles of NIST and NSA with respect to providing guidance and control of computer security for civilian agencies.

Prior to the passage of P.L. 100-235 the NSA, which is part of the Defense Department, was authorized under National Security Directive 145 to oversee all federal computer security standards and training. NIST and NSA developed a Memorandum of Understanding (MOU) in order to work cooperatively in carrying out their responsibilities under the Computer Security Act of 1987. The MOU established the following agreement between the two agencies:

- Recognizes NIST's responsibilities for developing security standards for sensitive unclassified (non-national security) systems.
- NIST will draw upon NSA's expertise where appropriate.
- NIST will recognize trusted system criteria.
- The MOU establishes a technical working group to resolve issues.
- The MOU directs the agencies to exchange working papers.

Together, the MOU and the Computer Security Act resulted in giving responsibility for security standards to the National Institute of Standards and Technology, a civilian agency, and having the National Security Agency, a defense agency, play more of an advisory role for computer security of sensitive data.

The Computer Security Act of 1987 (P.L. 100-235), as enacted on January 8, 1988 requires specific computer security measures to be taken by federal agencies. These include:

1. Identifying computer systems that contain sensitive information
2. Establishing a plan for security and privacy of each federal computer system identified. Plans were to be submitted to NIST and NSA for advice and comments.
3. Providing mandatory periodic training in computer security awareness and accepted computer security practices for employees involved in each computer system

Congress continues to work on legislation and revision of bills in the areas of anti-virus, hacker prevention, privacy, and computer fraud. Hearings were held in December, 1989 to explore the provisions of several pending computer protection laws. Testimony was presented before the House Judiciary Subcommittee on two new bills to tighten the punishment for computer crimes as a deterrent to potential hackers.

Representative Tom McMillen of Maryland introduced the Computer Protection Act (H.R.287) to broaden the scope of computer-related

activities deemed as wrongful acts to computer systems and therefore subject to jail punishments. Representative Wally Herger of California proposed the Virus Eradication Act (H.R.55), which is the first legislative bill introduced to deal specifically with computer damage induced by a virus. Both H.R.287 and H.R.55, should they become law, are expected to extend the provisions of the 1986 Computer Fraud and Abuse Act, which centers on unauthorized access to computer systems such as illegally going into a bank's data base to transfer money.

Additional hearings are to be scheduled during 1990 for the proposed computer security legislation. Industry is urging Congress to act quickly to address the technical computer issues for amending the Computer Fraud and Abuse Act. Redefining access to computer systems to address networks, laptops, and voice mail systems is being sought, along with other software-related developments to combat viruses.

There have been several other pieces of legislation over the past 20 years that related in some way to computer security:

- The Electronic Communications Privacy Act of 1986 protects against unauthorized interception of electronic communication, updating the 1968 voice-oriented wire tap law.
- The Electronic Funds Transfer Act of 1978 establishes criminal penalties for computer system stealing through a fraudulent transfer of funds.
- The Privacy Act of 1974 establishes criminal penalties for transferring personal information from a government data base, except under specific authorization.

F
Key Federal Agencies

In addition to the Congress, many other agencies play an active role in computer security. This section discusses the activities of some of these agencies.

1. General Services Administration (GSA)

The General Services Administration (GSA) plays a somewhat narrow role in the regulation of computer security. It is the responsibility of the GSA to issue policies and regulations for the following areas:

1. The physical security of computer rooms consistent with the standards and guidelines issued by NIST
2. Agency procurement requests for automated data processing equipment, software, and related services to include security requirements
3. Procurements made by GSA to meet the security requirements established by the user agency

The Federal Information Management Regulation (FIRMR) issued by GSA provides guidance for the acquisition and management of information resources. FIRMR guidance in 41 Code of Federal Regulations, Chapter 201 includes security for information systems under development. The automated information system development and management requirements in OMB Circular A-130 and the FIRMR are similar. For example, the FIRMR requires that federal agencies establish an adequate security program "to ensure automated information integrity; i.e., a security program that

a. Ensures that under all conditions, sensitive data is safeguarded from disclosure and protected from unauthorized modification or destruction,

b. Provides for operational reliability of ADP and telecommunications systems, and

c. Provides asset integrity for prevention of loss from natural hazards, fire, etc."

In addition, GSA's Office of Technical Assistance (OTA) has published a guideline entitled "Information Technology Installation Security."

2. Office of Management and Budget (OMB)

Under the training provisions of the Computer Security Act of 1987, OMB is directed to issue regulations prescribing the procedures and scope of the training to be provided to federal civilian employees. OMB is also to issue regulations indicating the manner in which training is to be carried out.

The training regulation OMB issued in 1988 focused on employee awareness of system vulnerabilities and risks. Federal employee training is to be a continual process at agencies. According to OMB, training will include non-classroom methods, such as videos and manuals.

Also in 1988, OMB published guidelines for agencies to use in preparing computer security plans. The OMB guidelines require agencies to document security awareness and training programs for their major application and support systems.

Additional security guidance from OMB is available to agencies in OMB Circular No. A-130. Under this circular, OMB is authorized to review agencies' policies, practices, and programs pertaining to the security, protection, sharing, and disclosure of information, in order to ensure compliance with the Privacy Act and other related statutes.

Although not directed solely at security practices, Circular A-130 contains agency responsibilities and practices that must be considered during system development in the area of information security. Specifically, OMB Circular A-130 states that agencies shall assure the following:

1. That automatic information systems operate effectively and accurately

2. That these systems incorporate appropriate technical, personnel, administrative, environmental, and telecommunications security controls

3. That the continuity of operations of informations systems that support critical or sensitive agency functions be maintained

OMB is also expected to publish a new circular on computer security planning.

3. National Security Agency (NSA)

The National Security Agency was established by presidential directive in 1952 as a separately organized agency within the Department of Defense. NSA was charged with the mission of computer security under a 1984 presidential directive. The agency has the following responsibilities:

- Prescribing certain security principles, doctrines, and procedures for the U.S. government

- Organizing and coordinating the research and engineering activities of the federal government in support of the agency's assigned security mission

- Operating the National Computer Security Center (NCSC)

- Conducting security product evaluations/certifications (Evaluated Products List)

As noted earlier, NSA and NIST entered into a Memorandum of Understanding regarding the security of sensitive data. The Computer Security Act further specified that the technical advice and assistance of the National Security Agency shall be called upon where appropriate. NSA and NIST jointly reviewed the thousands of computer plans from the federal agencies. The plans were returned to the agencies along with comments and suggestions.

NSA's influence on the federal computer security market is most visible through its establishment of categories for levels of security (A to D) for systems as defined in the DoD Trusted Computer System Evaluation

Criteria (the "Orange Book"). The National Computer Security Center evaluates and certifies computer systems according to seven levels of security. These were summarized in Section III.A and Appendix D describes each level in a brief narrative.

The federal agencies are striving to achieve the C2 level by 1992 as called for in Defense Directive 5200.28. Vendors such as Digital, Unisys, IBM, Hewlett-Packard, and Wang are offering products at the C2 level with optional upgrades to B1 and A1 for some products. Industry has hardware, software, dial-back modems, and encryption devices in the federal marketplace that have already passed Orange Book criteria for testing. This process can take several years, depending on the capabilities and complexity of the security product. Although no requirements exist for public key crypto, INPUT expects NSA to foster a digital signal standard. NSA is working with industry to strengthen the vendor's understanding of the DoD security standards, features, and procedures for obtaining ratings for secure systems. The aim is to achieve improved consistency in products.

4. National Institute of Standards and Technology (NIST)

NIST (formerly the National Bureau of Standards) is an operating unit of the Department of Commerce. The agency's computer security mission is to:

- Develop and maintain security standards
- Assist federal agencies by providing advice and guidance in the use of standards
- Assist other agencies in specific systems development efforts
- Assist the private sector in using standards
- Conduct computer security-related research and studies

These responsibilities are reinforced by the Computer Security Act of 1987.

NIST together with NSA established computer security standards for civilian agencies and reviewed the computer security plans submitted by federal agencies. From NIST's perspective, the reviews identified weaknesses in agency awareness and training for security. Furthermore, NIST—in conjunction with DoD, Justice, and NSA—coordinates agency responses to computer security incidents and maintains a clearinghouse for security issues.

The National Computer Systems Laboratory operates under the direction of NIST to conduct research and be a liaison with industry. Exhibit III-10 is an organizational chart from the Laboratory. According to the Associate Director for NCSL, Lynn McNulty, the organization is concerned with a variety of security issues including integrating security with the utilization of GOSIP, and developing protection for networks and operating systems. Along with OMB and NSA, NIST will begin agency visits to investigate compliance with security requirements.

National Computer Systems Laboratory

Director
James H. Burrows
301/975-2819

Associate Director, Computer Security
Lynn McNulty
975-3241

Voluntary Standards Liaison
Robert E. Rountree, Jr.
975-2826

Program Coordination and Support Group
Shirley M. Radack
975-2833

Information Systems Engineering Division
David Jefferson
975-3262

- Data management technology
- Computer graphics
- Knowledge-based systems Software standards validation

Systems and Software Technology Unit
Allen Hankinson
975-3290

- Software development and maintenance methodology
- Office systems engineering
- Portable operating systems
- PC network technology and
- applications

Computer Security Division
Stuart Katzke
975-2934

- Security management
- Security technology
- Network security architectures
- Evaluation and validation techniques

Systems and Network Architecture Division
Kevin Mills
975-3643

- Formal methods for protocol development
- Network applications
- Network management
- Network protocols

Advanced Systems Division
Shukrl Wakid
975-2900

- Automated recognition techniques
- Parallel processing
- Advanced communications
- Computer storage media
- Automated information systems

During 1989, NIST formed a twelve-member Computer System Security and Privacy Advisory Board within the Department of Commerce. The Board's Chairman is James H. Burrows, director of NIST's Computer Laboratory. The duties of the Board according to the Computer Security Act are as follows:

1. To identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer security and privacy

2. To advise NIST and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems

3. To report its findings to the Secretary of Commerce, the Director of OMB, the Director of NSA, and the appropriate committees of Congress

Membership on the Board includes both federal government officials and industry representatives who are eminent in the fields of computer and telecommunications technology.

NIST, in its role as an agency of the Commerce Department, is also involved in another dispute. The Advisory Board wants to relax export controls on cryptographic equipment, but NSA opposes this. NIST is working with Congressional committees to take a fresh look at embedded cryptography and determine if new legislation is needed.

5. General Accounting Office (GAO)

The General Accounting Office has issued more than two dozen reports on federal computer security within the last five years. For example, in February, 1989, GAO issued a highly critical report on federal compliance with the training requirements of the Computer Security Act. In another report, written before the Internet virus incident, GAO warned that most agencies, while expanding their computer systems, are not paying enough attention to security. In still another report, which accompanied Congressional testimony given in July, 1989, GAO commented on the Internet virus, the factors facilitating it, the system vulnerabilities, and the factors hindering prosecution.

GAO's reports on computer security are not limited to criticisms. Some reports offer guidelines on managing security. One report, for example, offered suggestions for integrating computer security into other agency IRM functions. Another report made organizational suggestions to help agencies cope with the computer security threat. This included the establishment of a security "focal point" for interagency networks.

6. President's Council on Integrity and Efficiency (PCIE)

The PCIE, an interagency organization, did a survey of federal agencies' attention to computer security and compliance with the Act. The report criticizes agencies in the following areas:

- Technical Security Software Controls
  - Critical system files not adequately protected
    - Sensitive utility programs not adequately controlled
    - Tape bypass label processing not adequately restricted
  - Special security exposure interfaces not installed
- Administrative Security Controls
  - Security not administered by independent staff
    - Adequate policies, standards, and procedures not promulgated
    - Security violation reports not effectively reviewed

G

Federal Computer Security Vendors

In responding to federal computer security requirements the vendor community has developed a variety of products and services, some operating in classified environments. No single vendor dominates the market, and perceptions differ among agencies and vendors.

Exhibit III-11 lists the vendors which agency respondents mentioned most frequently, as well as others mentioned. Exhibit III-12 lists similar response information from the vendors. Unlike the agency responses, which showed little in the way of priority, the vendor responses showed a definite pattern. It should be noted that, though Digital ranked first among vendor responses, it was not even mentioned by agency respondents. This suggests that Digital needs to improve its security image with federal agencies.

The remainder of this section highlights some of the products that vendors provide to meet federal computer security needs.

EXHIBIT III-11

Agency Views—Leading Vendors in the Federal Computer Security Market

- Vendors mentioned most frequently
  - Comsis
  - Honeywell
  - IBM
- Other vendors mentioned
  - AT&T
  - CDSI
  - Computer Associates
  - EDI Audit
  - Fischer International
  - Grumman
  - Mainframe Incorporated
  - MMDS
  - SDS
  - TRW
  - U.S.S.

Note: 35% of agency respondents were unfamiliar with specific companies or nonresponsive to question.

EXHIBIT III-12

Vendor Views— Leading Federal Security Vendors

Vendors	Rank*
Digital Equipment Corporation	1
AT&T	2
IBM	3
Honeywell	4
Motorola	5
TRW	5
Xerox	6
Computer Associates	6
Unisys	6
Boeing Computer Services	7
Sun Microsystems Inc.	7
Trusted Information Systems	7

*Rank based on frequency of mentions by industry respondents.

1. Hardware Vendors

Most of the hardware market concerns Tempest-certified computers. Tempest certification relates to the features on some machines that are designed to limit low-level radiation emissions which are susceptible to eavesdroppers. Exhibit III-13 lists some of the leading Tempest vendors. For the most part, the list does not contain household names. Rather, it contains mostly companies that specialize in this market.

EXHIBIT III-13

Tempest-Certified Computers

Vendor	Equipment Market
Atlantic Research	Macintosh
CPT Corporation	Multiuser UNIX (Motorola Chip)
	AT-compatible (Intel Chip)
CR International	AT-compatible
Data General	Eclipse
Datasec	AT-compatible
	Macintosh
Datawatch	Multiuser UNIX (Intel Chip)
Delta Data	AT-compatible
	PS/2-compatible
Digital Equipment	VAX
Grid	Intel Chips
Hetra	AT-compatible
Hewlett-Packard	Vectra
International Technology	AT-compatible
	PS/2-compatible
Mesa Technology	AT-compatible
Mitek Systems	Macintosh
Tempest Technologies	AT-compatible
Wang	AT-compatible
	VS minicomputer
Zenith/Inteq	AT-compatible
	OS/2-compatible

In addition to its secure Macintosh, Mitek is also developing a Tempest version of Cygnet's optical mass storage products. The product is referred to as an optical jukebox. Some other computer security products include:

- Minatronics provides a fiber optic cable device for physical protection of microcomputers.
- Eye Dentify provides retinal scanning devices for use in access control systems.
- American Computer Security Products provide a product called Immune System, which it refers to as a "virus-proof" 286-based microcomputer.

2. Software Vendors

Far more software vendors participate in the federal computer security market than do hardware vendors. This reflects both the perception of more software opportunities as well as the (usually) lower capital investment required. The majority of software products fall into two categories:

- Products which aim at specific NSA security levels, as defined in the Orange Book.
- Products aimed at controlling access and protecting computer systems from viruses.

Some of the products having current or pending NCSC certification are listed in Exhibit III-14. Because of the cost of time required for NCSC certification, some vendors are asserting "Orange Book" compliance without certification. Although this will not help in the federal market, it may be useful in some commercial activities.

The version of a software product is critical to its security reliability. For example, while VAX/VMS was certified for the 4.3 version, the 4.4 version contained a flaw which permitted access to NASA's Space Physics Analysis Network. The technical complexity associated with security verifications has led to some confusion among both agencies and vendors. INPUT does not expect clarification any time soon, as some agencies look for ways to short-circuit the system.

EXHIBIT III-14

NCSC-Certified Products

Vendor	Product Names	Security Level
AT&T	UNIX System V/MLS	B1
IBM	VM/SP - RACF	C2
Digital	VAX/VMS Version 4.3	C2
Gould	UTX 32	Unknown
Sun	SUN OS/MLS	Pending
Harris	CS/SX	Pending
Unisys	OS 1100	B1
Trusted Information Systems	Trusted Xenix (formerly IBM's Secure Xenix)	B1
Sybase	Secure SQL Server	Pending
Microsoft	OS/2	C2

The second major category of security software products relates to virus and access protection. Exhibit III-15 lists some of the key products in this area. The wide variety of (relatively) unknown products suggests that some industry shakeout is likely, particularly for products protecting microcomputers.

EXHIBIT III-15

Access/Virus Protection Security Products

Vendor	Product Name	Operating Environment
American Computer	Compusec II	Intel MS-DOS
	Immune	Intel MS-DOS
Bourbaki	Muscle	Intel MS-DOS
CH Systems	Sleuth	
Commcrypt	Cryptolock	Intel MS-DOS
Computer Associates	CA-Unipack/SCA	MVS
CXR Telecom	AJ Series	
Cylink	CIDEC-LS/HS	
	Secure PC	Intel MS-DOS
Dial-Guard	Dial-Guard	VAX, Tandem,
Digital Pathways	Defender II, SLS	MVS
Enigma Logic	PC-Safe II	
	VAX-Safe	Intel MS-DOS
	UNIX-Safe	VAX VMS
	Stratus-Safe	UNIX
	Tandem-Safe	VOS
	Virus-Safe	VOS
First Aid Software	Anti-Virus Kit	Intel MS-DOS
Fischer International	Watchdog	Macintosh
Foundation Ware	Certus	Intel MS-DOS
Harcom Security	PC-Watchman	Intel
HJC Software	Virex	Intel MS-DOS
International Security Technology	Virus-Pro	Macintosh
Jones Futurex	ENC-3XX	Intel MS-DOS
Kent Marsh	Nightwatch	Intel MS-DOS
Kinetic Software	Access	Macintosh
Lattice	Secret Disk	Intel MS-DOS
LeeMah Datacom Sec.	Traqnet 2000	Intel MS-DOS
	Infokey	
Paul Mace Software	Mace Vaccine	
Panda Systems	Dr. Panda Utilities	Intel
PE Systems	Guardsman 100	Intel
	Gillaroo	
Pyramid Development	PC/DACS	Intel MS-DOS
Racal/Guardata	PCSM	Intel MS-DOS
Racal/Vadic	VA930, 4492	Intel MS-DOS
Rainbow Technologies	Data Sentry II	Intel
RG Software Systems	Disk Watcher	Intel
	Vi-Spy	Intel MS-DOS
RSA Data Security	MailSafe	Intel MS-DOS
	RSA Sign/Check	Intel MS-DOS
Software Concepts Design	Flu Shot	Intel
Software Directions	Soft Safe	Intel
Technical Communications	Cipher X, CSD 3324A	
	DSD 72A SP, CSD 909	
	Raven, The Key	
Triton Products	Virus Guard	Intel
Telco Systems	Accelerator	
Worldwide Software	Vaccine	Intel

3. Network Security Vendors

Network security has received more media attention, although not necessarily more federal funding, as a result of the 1988 Internet virus. However, it is widely believed that local-area networks (LANs) pose greater security problems. As might be expected, a wide range of vendors are offering network security products to federal customers:

- Electrospace Systems, Inc. has supplied more than $100 million worth of security telephones to the Air Force Logistics Command. GAO has suggested that some overcharging might be involved in the sale.

- Newbridge Networks offers a single chip encryption device, the CA3YC168 Digital Encryption Processor, that gives 150 kilobit/second throughout over TI telephone lines.

- Harris Computer Systems provides a product called LAN/SX, which is Verdix's secure LAN ported to the Harris secure UNIX operating system.

- Xerox provides the Xerox Encryption Unit (XEU), which allows both classified and unclassified information on the same LAN. It is activated by an electronic key insertion.

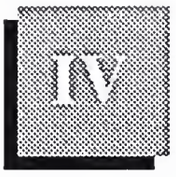
- Intel provides an encryption/decryption device entitled iKGM-100, a key generation module intended for use in computers, terminals, workstations, and smart peripherals. It uses an NSA design referred to as Tepache.

- In additional to its Harris porting, Verdix recently added a high-level VAX interface to its network security system. The interface, referred to as VIbus, has been added to the hardware and firmware security components applied to Ethernet LANs.

- Mika L.P. provides a hardware-based encryption device, entitled Whisper, for PC-based data security. It uses ordinary telephone lines and Hayes-compatible modems.

- 3COM Corporation has improved the security features on the network control servers it provides to the Air Force under the Unified Local Area Network Architecture (ULANA) contract.

In additional, the Corporation for Open Systems is attempting to speed the development of network security standards.



Federal User Requirements and Trends

This section describes the results of INPUT's survey of federal agencies, as well as other agency information reflecting requirements and trends in computer security.

In general, agency responses show a wide mix of opinions on present and future needs for computer security. Although everyone agrees on the need for network security, a plurality of respondents showed no established criteria for evaluating security products. This suggests some flexibility for vendors in responding to federal security needs. The market is not yet clearly defined.

However, a majority of agency respondents do not view past and current vendor efforts as successful. This suggests that at least some vendors need to change something in order to gain agency confidence. In particular, agencies mentioned delivery and support experience as areas where vendor improvement is needed. Vendors will also need to market heavily in order to overcome agency budget constraints and enhance market penetration.

A Federal Agency Compliance with Computer Security Act

During the 1989 survey of federal agencies, INPUT asked what security measures the agencies had adopted to date pursuant to the Computer Security Act of 1987. Exhibit IV-1 identifies the measures already completed. The largest percent (86%) noted that their agencies had identified their sensitive systems. The percent reporting that systems were identified, 86%, probably reflects the entire government fairly accurately. As GAO has reported, most agencies made a legitimate effort to identify their systems. However, INPUT's sample probably reported a higher ratio of plans implemented to plans completed. The GAO looked at security controls in 22 plans, and found that only 38% of those planned had been implemented. This suggests business opportunities for vendors who can help agencies implement the plans.

Under the Computer Security Act, sensitive systems were to be identified by July 8, 1988. Agencies could then proceed to establish a security plan for each federal system that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access or modification of the information contained in the system. Furthermore, according to the Act, a summary of the plan should be included in the agency's five-year plan.

As noted in Exhibit IV-1, sixty-eight percent of the agency respondents reported that they had completed the required security plans due to NIST by January 9, 1989. NIST reported receiving 1,000 plans, or approximately half of those required, by the deadline. OMB is responsible for ensuring that agencies have appropriate security plans in place; NIST and NSA handle review and evaluation of the plans. The plans ranged from one page to over 200 pages and addressed a variety of policy and procedural issues. The preliminary reviews by NIST and NSA indicated some shortcomings in awareness and training which will need to be taken up in future year submissions, if new plans are submitted.

During 1989, 41% of the agency respondents indicated implementation of the security plans. Many agencies have begun training their employees in computer security awareness, while other federal agencies are still establishing security policies. The implementation phase varies among agencies due to the differing nature of security and number of sensitive computer systems at each site.

EXHIBIT IV-1

Computer Security Measures Adopted

Security Measure	Percent of Respondents*
Sensitive Systems Identified	86
Security Plans Completed	68
Security Plans Implemented	41

*Adds to more than 100% due to multiple responses.

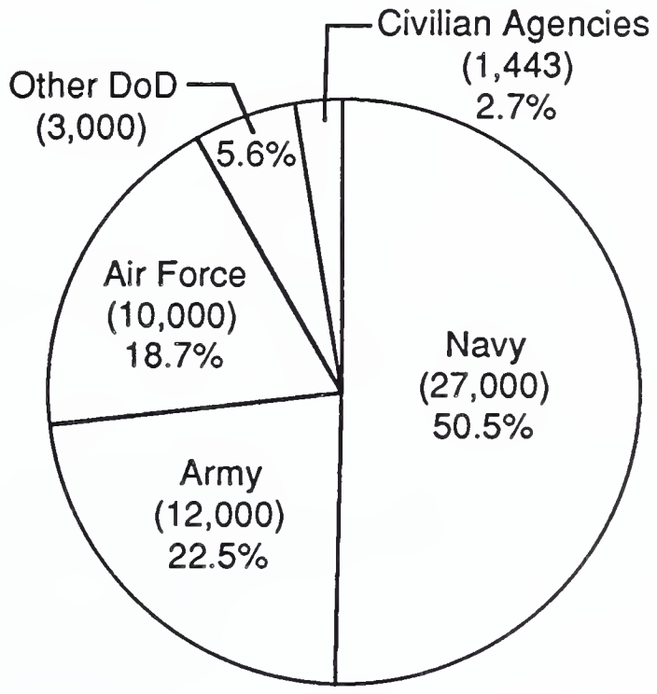
The General Accounting Office (GAO) studied the compliance of the federal agencies in reporting the number of installed sensitive systems. Seventy-two agencies responded to the GAO inquiry. The total number of sensitive systems identified by the agencies reached 53,443 as of September 8, 1988. Exhibit IV-2 displays the number of systems for selected agencies and the proportion each represented of the total reported. The defense agencies reported an estimated 52,000 sensitive

systems or about 97% of the total reported by all government agencies. The Navy, with 27,000 systems, is the single largest agency for sensitive systems.

Further research shows that many civilian agencies aggregated their systems, thus reducing the total number. Defense agencies, however, did not consolidate, which drove up their numbers. This suggests that vendors may pursue far more than the 53,000 systems that GAO identified.

EXHIBIT IV-2

Number of Sensitive Systems Reported by Agencies as of September, 1988



Total Reported by 72 Federal Agencies = 53,443 Sensitive Systems

Source: Computer Security, Status of Compliance with the Computer Security Act of 1987, Briefing Report to Congressional Requestors, GAO, September, 1988.

Exhibit IV-3 illustrates the respondent views of the responsibilities of government agency staff for implementation of security measures. Nearly half (47%) of the staff are directly responsible for agency efforts for the design/implementation of policies. Under the Computer Security Act, each agency may employ computer security standards which at a minimum contain the standards made compulsory by NIST. Thirty-five

percent of the respondents have total responsibility for computer security at their agency. It is viewed as advantageous for some agencies to centralize computer security responsibility in one office. Additional responsibility areas for agency personnel include oversight of adherence to standards and general management.

EXHIBIT IV-3

Agency Staff Responsibilities for Security Implementation

	Percent of Respondents
Design and/or Implement Security Policies/Guidelines	47
Total Responsibility	35
Ensure Adherence to Standards and Directives	12
Security Manager for Staff	6

In February, 1989, GAO published a report entitled, "Compliance with Training Requirements of the Computer Security Act of 1987." The GAO surveyed 85 agencies in connection with training progress, and found the following:

- 45 agencies have initiated computer security training.
- 19 agencies plan to start a training program.
- Two agencies could not say when they would start training.
- 15 agencies claimed that they have no sensitive systems.
- Four agencies did not respond to the survey.

B

Future Computer Security Measures

In the future, more rigorous security programs and training will be needed by the federal agencies to protect the integrity and privacy of information systems. Agency program managers are slowly gaining experience in establishing security requirements and developing plans. This should move the federal agencies closer to compliance to all provisions of the Computer Security Act.

Exhibit IV-4 reflects agency responses to questions about computer security measures planned for the next two to five years. The largest

number (37%) of the respondents plan to implement security features in their computer software. In order to meet the agencies' needs, industry is developing modifications to DBMS products to meet B2 requirements, and network-based software to handle multiple-level access.

EXHIBIT IV-4

Future Computer Security Measures

Security Measure	Percent of Respondents*
Implement Security Features in Software	37
Increase Security Training/Awareness	32
Implement Other Security Measures	27
Develop Contingency Plan	18
Conduct Risk Analysis	14

*Adds to more than 100% due to multiple responses.

Increased computer training and awareness will be undertaken by nearly one-third of the respondents over the next few years. To assist the agencies in complying with training requirements, the Office of Personnel Management issued computer security awareness training material to agency managers. OPM will continue to work with NIST and an interagency advisory group to develop and distribute additional training aids.

The survey findings indicated a wide range of other planned security measures that accounted for 24% of the responses. These other measures include:

- Achieving C2-level functionality by 1992 for all systems and networks
- Enhancement of monitoring devices and access controls
- Hiring of security program managers
- Conducting security reviews
- Obtaining certification of system designs

The federal agencies are also attempting to develop their contingency plans and risk analyses. The contingency plans allow agencies to have in place established routines and procedures for activation in cases of security violations. Each plan describes the appropriate response to

situations which jeopardize the safety of data or information processing and communications facilities.

Risk analysis is an evaluation of system assets and vulnerabilities to establish an expected annual loss or equivalent for certain events, based on costs and estimated probabilities of the occurrence, or a ranking of the categories of risk of those events. The risk analysis should detect some of the serious security problems associated with federal information systems, thus allowing for installation of proper safeguards at the agencies. Controlled access, user authentication rules, passwords, encryption, and physical security controls are all options that need to be evaluated. Many agencies believe they should expedite the necessary risk analyses in order to ensure the security of their current and future systems.

To control its risk in the event of a catastrophic security violation, DoD is establishing a central, nationally based coordination center. This center will serve as a focal point for operating and investigative personnel in the event of a computer network emergency. The center will:

- Establish continuing contacts with technical experts from industry and universities
- Receive problem reports
- Authenticate correction sources
- Provide public information on a virus attack

Another security measure being taken with more frequency involves the procurement process. Many solicitations now have clauses relating to Contractor-Induced Computer Viruses (CICV). This puts the burden and risk on contractors to insure that all delivered products are virus-free. Many solicitations now contain clauses which:

- Notify contractors that they are responsible for CICVs and that liability will be addressed under both the FARs and the FIRMRs
- Require proposals to identify the approach(es) for preventing CICVs
- Provide inspection and acceptance test clauses and CICV-free warranties

C

Vulnerability of Federal Computer Systems

Federal agencies' information systems are vulnerable to the harmful effects of natural and human-made hazards, which can impact the accuracy, integrity, and continuity of computer operations. Even with installation of mechanisms and techniques that control access to stored information, the physical and operational aspects of information systems lead to their vulnerability.

In a published report, Congressman Wally Herger indicated the presence of system vulnerabilities at NSA, the SDI office, EPA and the House of Representatives. In each case, computer virus penetration demonstrated the weaknesses of agency computer systems. The report also highlights the need to improve computer security at nuclear power plants and air traffic control centers.

Exhibit IV-5 shows the agency respondent views on which computer systems are most vulnerable to security problems. Microcomputers were named twice as often as either mainframes or midsize systems. The federal government has nearly 500,000 microcomputers in its inventory; thus the magnitude of potential computer security problems is huge.

EXHIBIT IV-5

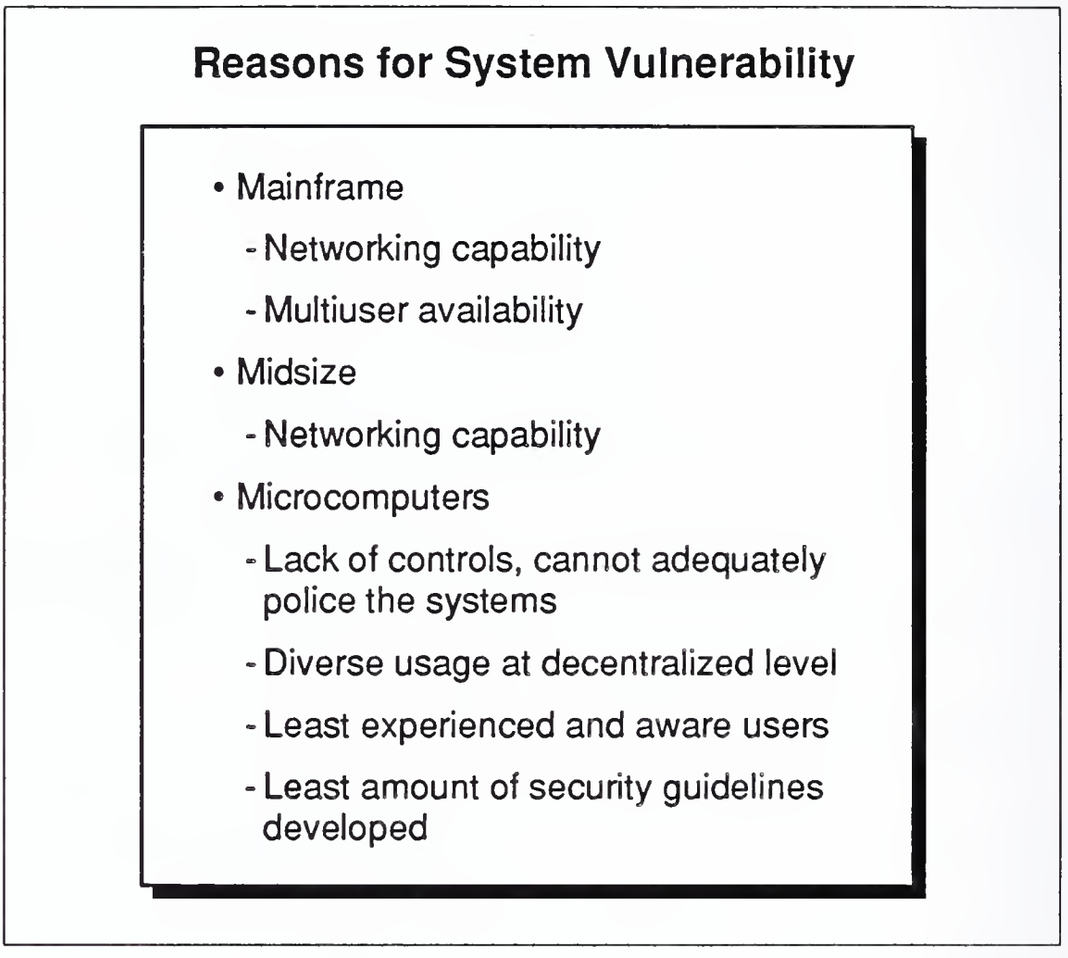
Systems Most Vulnerable to Security Problems

Type	Percent of Respondents*
Microcomputers	64
Mainframes	36
Midsize	36

*Adds to more than 100% due to multiple responses.

The networking capability of both mainframes and midsize systems is the most common reason for these systems' vulnerability, as is noted in Exhibit IV-6. Mainframes are also vulnerable because of multiuser availability. Greater system accessibility by a larger number of potential users substantially increases the risk for unauthorized manipulation of data and potential invasion of viruses. The respondents mentioned that security limits of gateways and network controllers leave systems vulnerable. Furthermore, the ability to access networks via telecommunications increases the risks of altered or destroyed data.

EXHIBIT IV-6



The widespread use of microcomputers has exceeded the level needed for adequate control and policing of security policies for users. To compound the problems, usage is also decentralized. Geographically dispersed government sites with diverse functional/application areas contribute to the difficulties in regulating and developing standards and guidelines for the security of microcomputer systems. In addition, respondents mentioned that micro users may not be as highly trained and aware of security measures. Less experienced users would not often detect irregularities or report unauthorized computer practices.

The agency respondents were asked to identify the major security threats to computer systems. The multiple responses are summarized in Exhibit IV-7. Seventy-four percent of the respondents indicated that data access was the main area of potential threat. This coincides with the agencies' heightened interest in password security and user authentication techniques.

EXHIBIT IV-7

Perceived Computer System Threats

System Threat	Percent of Respondents*
Data Access	74
Data Manipulation	42
Software or System Manipulation	42
Site Access and Damage	21

*Adds to more than 100% due to multiple responses.

Data, software, or system manipulation were mentioned as perceived threats by 42% of the respondents. Manipulation by unauthorized sources can result in the loss of information, compromise of the accuracy/integrity of data and illegal access to sensitive information. Only 21% of the responses indicated that site access and damage was a serious threat. Apparently, physical entry of facilities and destruction of records or equipment is not seen as much of a reality for some agencies, or precautions such as security guards, locked areas, and restrictive entry have already been implemented. Lack of access control, especially during non-working hours, was highlighted by GAO as a major security defect in the early 1980s.

The agencies were also mindful of the impact of increased end-user computing. Respondents noted an increased vulnerability to data manipulation and other security risks arising from the increase in end-user computing. Also mentioned was a need for increased awareness and security training for the users. Furthermore, agency respondents see a need to supplement the security regulations specifically for micros.

FTS 2000 will do little to improve the security of end-user computing. It was not intended to be a secure network. However, both AT&T and Sprint are required to provide detailed call records as well as controls on access to the records. These controls are expected to meet C2 requirements, as defined in the Orange Book.

D

Protective Measures and Guidelines for Security

1. Agency Security Measures

Agencies need to rapidly move toward implementation of computer security measures in order to comply with already established and evolving security guidelines. The consequences of inadequate security controls in government systems are likely to become increasingly important in the future. The federal government has been expanding its dependence on automated information systems to maintain and process a range of mission-critical, sensitive information. With increased government dependence on information systems and decentralized processing, government automated information systems will be subject to an increased range of vulnerabilities.

The Computer Security Act of 1987 requires the formulation of comprehensive security awareness and training programs for government agencies. Agencies must disseminate to their employees information on security requirements and safeguards that are critical to each agency's mission and operation of computer systems.

As shown in Exhibit IV-8, the survey findings indicated that less than half (45%) of the respondents were educating users and increasing security awareness as steps to protect their computers from viruses and other security violations. A substantial number of the respondents were not concerned with the use of properly authorized software, even though virus-infected software can quickly infiltrate a network. Only eighteen percent of the respondents specified intentions to implement an anti-virus software program. The cost of changing software over the life cycle of a system is an important hurdle that agencies must overcome in addressing technical software-related security issues, such as access control.

The other security measures cited by the respondents included the following:

- Improve network monitoring
- Disallow bulletin boards
- Develop emergency response procedures
- Add layered security down to department level

The Bureau of Labor Statistics installed special software that generates secure digital signatures. The Bureau has 1,800 users on a 3COM Corporation network, connecting four Washington area sites with eight

EXHIBIT IV-8

Measures Taken to Secure Computer Systems

	Percent of Respondents*
Educate Users/Increase Awareness	45
Use of Authorized Software Only	18
Issue Guidelines/Strategies	18
Implement Anti-virus Software	18
Other	18
Publish Alerts to Virus Outbreaks	9

*Total greater than 100% due to multiple responses.

regional offices. From BLS' point of view, common software errors and natural disasters present a greater threat to data integrity than does malicious tampering. The digital signature approach also helps BLS to expedite its problem resolution activities.

2. Training Programs

Section 5 of the Computer Security Act states that each federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each federal computer system. Such training shall be provided in accordance with regulations established by NIST and OPM prescribing the procedures and scope of training for federal civilian employees.

INPUT received diverse responses from the agencies on computer training initiated to date. Many respondents have introduced general security awareness training, while others are conducting more limited seminars and briefings on security issues. The majority of survey replies can be classified as either general instruction or targeted to specific personnel/user groups as follows:

General Instruction Training
- Internal seminars
- Annual security awareness bulletins
- Unit monitoring
- Classes conducted on a regular basis

Agency Personnel/ User Group Training
- New employees/ Introductory level
- Supervisory staff (managers and officers)
- User training for security rules
- Employee training for accessing sensitive data

The majority of respondents did not believe that employee awareness of computer security required any additional training. However, the agency representatives did note an increased demand for end-user microcomputer controls and larger training requirements arising from the increased use of microcomputers. Updated training is also needed for newer computer technologies as well as more in-depth training in general.

Under Section 5 (b) of the Computer Security Act, training must start within 60 days of the issuance of the OPM training regulation required in Section 5(c). OPM issued its interim training regulation on July 13, 1988; therefore the deadline was September 11, 1988.

In December, 1988 GAO requested information from agencies on the status of their compliance with sections 5(a) and 5 (b) of the law. A total of 81 agencies responded to GAO and the findings are summarized below:

- 45 agencies reported starting their computer security training program as required by the Act.

- 19 agencies reported plans to start the training programs between November and April, 1989.

- 2 agencies reported no set plans for the training program at that time.

- 15 agencies stated that they had no computer systems containing sensitive information.

The GAO report also reviewed the training tools used by the agencies. Thirty-one of the 45 agencies which had begun their training had a total of 190 different training courses and modules in use. Fifty-eight percent of the modules covered computer security basics, and 53% dealt with policies, procedures, and practices. Many of the 190 courses or modules were targeted to functional or program managers (56%), and at end users (50%). The training courses/modules also covered contingency planning and life cycle management.

3. Federal Agency Directives and Guidelines

Ninety-five percent of agency respondents report that they are adhering to their departmental computer security directives and regulations as shown in Exhibit IV-9. The exhibit also indicates the breakout of DoD versus civilian regulations for the responses, with civilian agencies having a larger share.

Over half (55%) of the agencies identified other directives and guidelines. There was an extensive variety of security guidelines cited. Those mentioned included the well-known publications such as the NSA's Orange Book as well as narrowly distributed defense agency security directives. OMB Circular A-130 was cited frequently since it contains the OMB security guidelines relevant to the development of automated information systems.

EXHIBIT IV-9

Computer Security Directives and Guidelines

Policy Document	Percent of Respondents*
Departmental Directives/Regulations	95
- DoD 43%	
- Civilian 57%	
Other	55
OMB-130	23
NIST	9

*Total greater than 100% due to multiple responses.

A surprising survey result included in Exhibit IV-9 is that only 9% of the responses acknowledged NIST's role in establishing security directives

and guidelines. The respondents' perceptions are that guidelines come from their department, not a higher government-wide source, such as NIST or GSA.

The Computer Security Act itself specifies that NIST shall have the responsibility for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in federal computer systems. NIST shall draw upon the guidelines developed by NSA and also coordinate efforts with other government agencies including DoD, GAO, OMB, and the Office of Technology Assessment.

Some agencies are resisting NIST's oversight, further aggravating the implementation of security procedures. It has been reported that many agencies are not identifying their sensitive systems, especially the LANs. A newly organized Federal ADP Users Group (FADPUG) Special Interest Group is aimed at helping agencies secure these systems, even if they have not been declared sensitive.

E

Functional Requirements and Performance Criteria

There is a broad spectrum of functional security requirements that can be applied to an information system. These range from the relatively inexpensive and uncomplicated (for example, use of passwords) to the technically challenging and very expensive (i.e., A1 certification from the National Computer Security Center). Selection of functional requirements can significantly affect system costs, complexity, delivery schedules and performance.

Agency respondents gave multiple responses in identifying their particular agency's functional security requirements, which are compiled in Exhibit IV-10. All respondents specified network security. This requirement arises out of the agencies' operating environments, which are comprised of a growing number of PCs and workstations in LANs. Vendors are working to add security products that are either embedded in a computer's operating system or are add-on security packages suitable for the federal government's various networks. The major concern of agencies is their ability to maintain security across different networks.

End-user access includes user authentication, which identifies the user and verifies the user's eligibility for accessing the system. Functional safeguards to assure limited and proper access to sensitive data include encryption techniques, passwords, and multilevel security operating systems.

EXHIBIT IV-10

Functional Requirements for Computer Security

Requirement	Percent of Respondents*
Network Security	100
End-User Access	95
Data Security	91
Physical Security	86

*Total greater than 100% due to multiple responses.

Functional requirements for data security were mentioned by 91% of the respondents. These requirements serve to protect the accuracy, integrity, and continuity of computer operations and processing of information for mission-critical and sensitive systems. Data security measures can utilize keys, passwords, log-on identifiers, and encryption techniques. Unresolved issues regarding data security include compliance with C2 requirements, porting to a security platform, and proprietary algorithms. Agencies will continue to add data security requirements to make their data tamper-resistant.

Eighty-six percent of the agencies cited physical security requirements. These include limited or restrictive access to computer centers, remote processing sites, or LAN or WAN sites. Physical security is often the least costly and easiest functional requirement to fulfill. Employment of security guards, locked entrances, and limited accessibility are several available options for reducing system vulnerability. Some agencies, such as the State Department, are pursuing increased education and training as the best way to foster computer security. With so many foreign nationals employed at American embassies, it is especially important that all personnel recognize the need for computer security.

It is generally recognized that the most efficient and effective means to assure that a system contains the appropriate security controls and functions is to address computer security issues during the development of the system. Moreover, in cases where the security features of a system are an important consideration, it may be especially difficult to retrofit security into a system after it is operational. If the functional nature of the system is defined before security concerns are specified, system functional characteristics may be inconsistent with appropriate security objectives. In other situations, it may be technically or economically impossible to

correct this problem. For example, certain security features, such as mandatory access control, may be difficult to retrofit into a system after the operational system and application software have been accepted.

Agencies will find it easier to build in security in the initial development phases. However, the problem remains of how to bring current information systems up to the level of security standards being mandated. For example, the IRS Tax System Modernization effort is forcing a rethinking of data security efforts. The agency is aiming for C2-level security in all its new mainline systems.

The federal agencies offered little comment on the performance criteria established for computer security products. Exhibit IV-11 indicates that 30% of the respondents have not yet established any criteria. One-fourth of the agencies interviewed are evaluating performance criteria in-house or at a departmental level. This method of evaluation tends to vary the expected performance among different agencies based upon their own information processing needs and types of systems, rather than promoting product uniformity.

EXHIBIT IV-11

Agency Performance Criteria for Security Products

Criteria	Percent of Respondents
No Established Criteria	30
In-house Evaluation/Criteria	25
Other Criteria	25
Control Access	20

The agencies' specification of controlled access to sensitive data and computer systems is indicative of their immediate demand for products that will protect information from outside manipulation and/or destruction. Products that establish appropriate procedures for access to networks, physical computer sites, and data bases each need to meet established agency performance criteria.

Additional performance criteria for security products mentioned by respondents include:

- Compliance with security architectures being drafted
- Low overhead costs
- Built-in software security
- Monitoring, auditing, and reporting capabilities
- Compliance with DoD C2 capabilities

Agency respondents evaluated the level of success for industry's satisfying the agency's current performance criteria. Exhibit IV-12 is based on agencies' present experience with various vendors. The levels of success ranged from very successful to not successful, with two midranges of compliance with performance criteria.

EXHIBIT IV-12

Agency Evaluation of Industry Satisfying Criteria for Security Products

Degree of Success	Percent of Respondents
Very Successful	27
Moderately Successful with Future Improvements Needed	20
Limited Success	40
Not Successful	13

Some respondents (27%) viewed the computer vendors as already being very successful in providing products which comply with their agency's performance criteria. However, the majority (60%) of respondents categorized industry as having moderate or limited success to date. Some of the respondents—who indicated a current level of moderate success, with future improvements needed—suggested improvements providing greater protection of application software, easier implementation, and avoidance of retrofitting.

F

Acquisition Plans and Preferences

1. Acquisition Plans

As shown in Exhibit IV-13, eighty-two percent of the respondents indicated that their agencies would be adding software-driven password security over the next few years. A large portion of respondents also indicated that additional training tools and secure networking products would be acquired. These additional computer security acquisitions will support the agencies' compliance with required security standards and lessen the vulnerability of agency network systems.

EXHIBIT IV-13

Security Acquired through 1993

	Percent of Respondents
Software-Driven Password Security	82
Security Training Tools	77
Secure Networking Products	68
Risk Management Analysis	59
Communications Security Products	55
Data Encryption Equipment	55
Other Contractor Support	50
Other Computer Security Devices	50
Contractor Assistance for Preparation of Plans	45
Secure UNIX-based Products	41
Secure Workstations	38
Tempest Products	27
Emission Control Devices	14

Over half of the respondents plan to acquire risk management analysis, communication security products and data encryption equipment. These services and products will further address the data security problems and end-user accessibility which are part of the major functional requirements for the security of information systems.

Although most of the agencies submitted their initial plans by the 1989 interview period, 45% of the respondents indicated planned use of contractor assistance for the preparation of computer security plans. Presently, a smaller portion of agencies are still in need of initial assistance. Future computer plans may require some degree of contractor support, but not as much as in the earlier period of agency planning.

As noted in Exhibit IV-13, fewer respondents indicated intentions to acquire secure UNIX-based products, secure workstations, or Tempest products. These products in some cases are just beginning to find their role in civilian agency applications. Furthermore, additional product development and enhancements are still occurring, which may account for a wait-and-see attitude among agency respondents.

2. Method of Acquisition

Agency respondents were asked to comment on the planned method of purchasing computer security products. The respondents gave multiple replies to the acquisition methods they will use, as shown in Exhibit IV-14. Multiple responses indicate that agencies expect to employ a variety of methods, depending on their particular needs.

EXHIBIT IV-14

Acquisition Methods—
Computer Security Products

Acquisition Method	Percent of Respondents*
GSA Schedules	85
RFP for Specific Purchase	60
RFP for Requirements Contract	55
Purchase Security Devices as Part of Other Procurements	40
Other Methods	20

*Total greater than 100% due to multiple responses.

Eighty-five percent of the respondents expect to buy from the GSA Schedule. GSA Schedule purchases will probably be used for agency purchases of software-related products and training tools, and additional items that are below approval thresholds. An almost equal share of respondents (60% and 55% respectively) indicated that their agency would use RFPs for a specific purchase or a requirements contract. There is a growing trend among federal agencies to use requirements contracts, and these may be extended into the computer security area.

Security products are also being acquired as part of other procurements. Respondents specified use of the Treasury TMAC and DMAC procurements as examples. Furthermore, respondents included in the other category generally use the open market and small business contracts.

The questionnaire also attempted to provide some indication of the trend approved in government agencies for acquiring the services of GSA-approved contractors to support their security needs. Thirty-two percent of the respondents stated that they already have or are planning to use a GSA contractor, and 45% of the respondents have no plans. The remaining 23% are undecided about the use of GSA contractor services.

Agencies that have already used contractors used them for risk analysis, planning, preparation of policies and guidance, and instruction implementation.

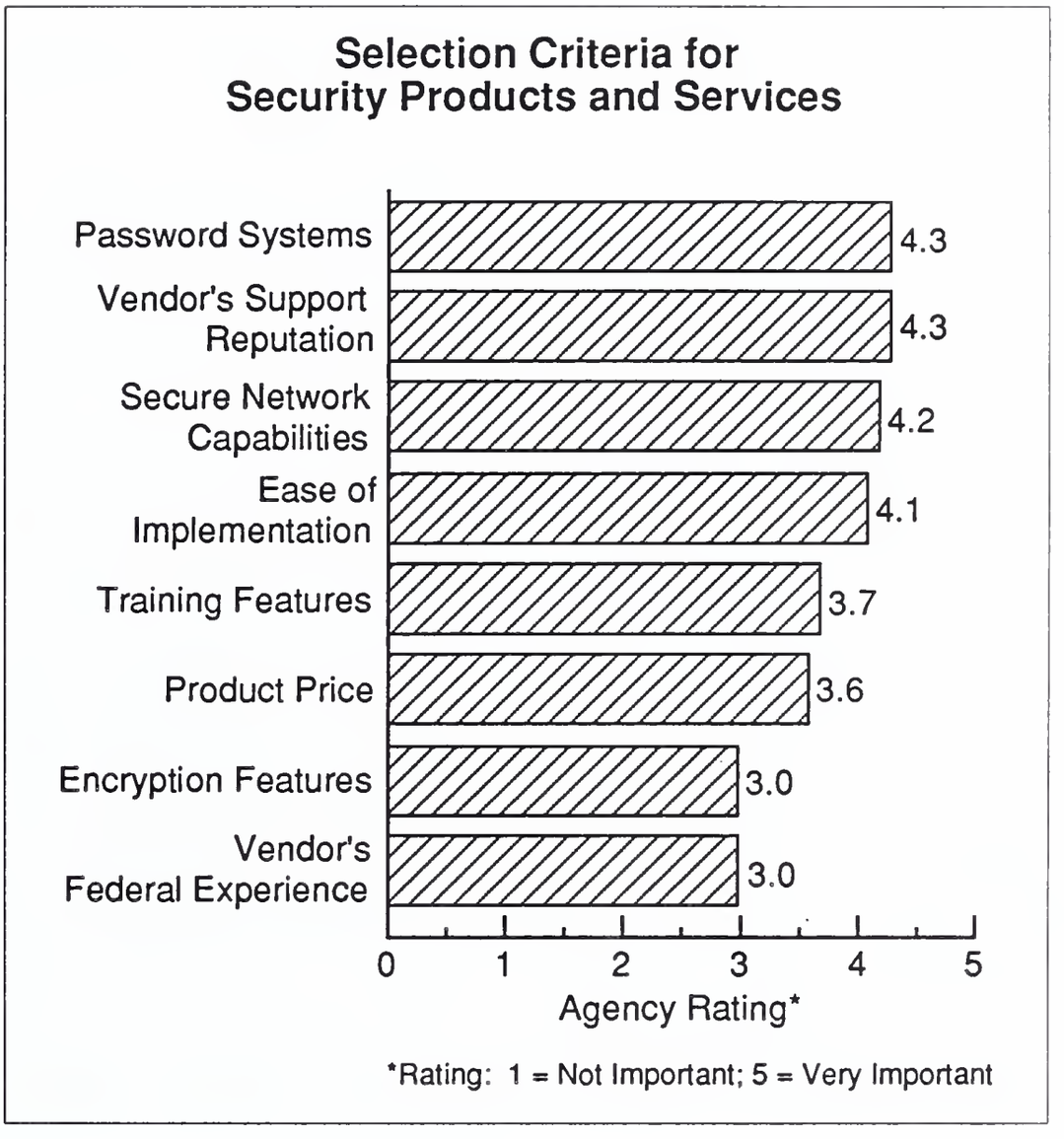
3. Product Selection Criteria

Agency ratings of the relative importance of various criteria in the selection of security products and services are shown in Exhibit IV-15. Password systems and vendors' support reputations tied for first place in importance. These two criteria reflect the current security emphasis at agencies, which need to install passwords that control access to systems. Agencies also focus on the reported support that vendors have been giving to their federal clients. A favorable reputation quickly spreads throughout the government, increasing the demand for products. A poor reputation is also passed on by word of mouth and is hard to overcome to capture additional federal sales.

The ratings for secure network capabilities and ease of implementation were also important factors for agencies and vendors. This again reflects the priority of agencies to resolve network vulnerability problems.

The extent of federal experience needed by the vendor was given the lowest rating by the agencies. Therefore, for selection of computer security products/services, the functionality and the positive support reputation of the vendor supersedes the vendor's government-related experience. In general, the ratings reflect a subtle shift in agency interest from performance to functional considerations.

EXHIBIT IV-15



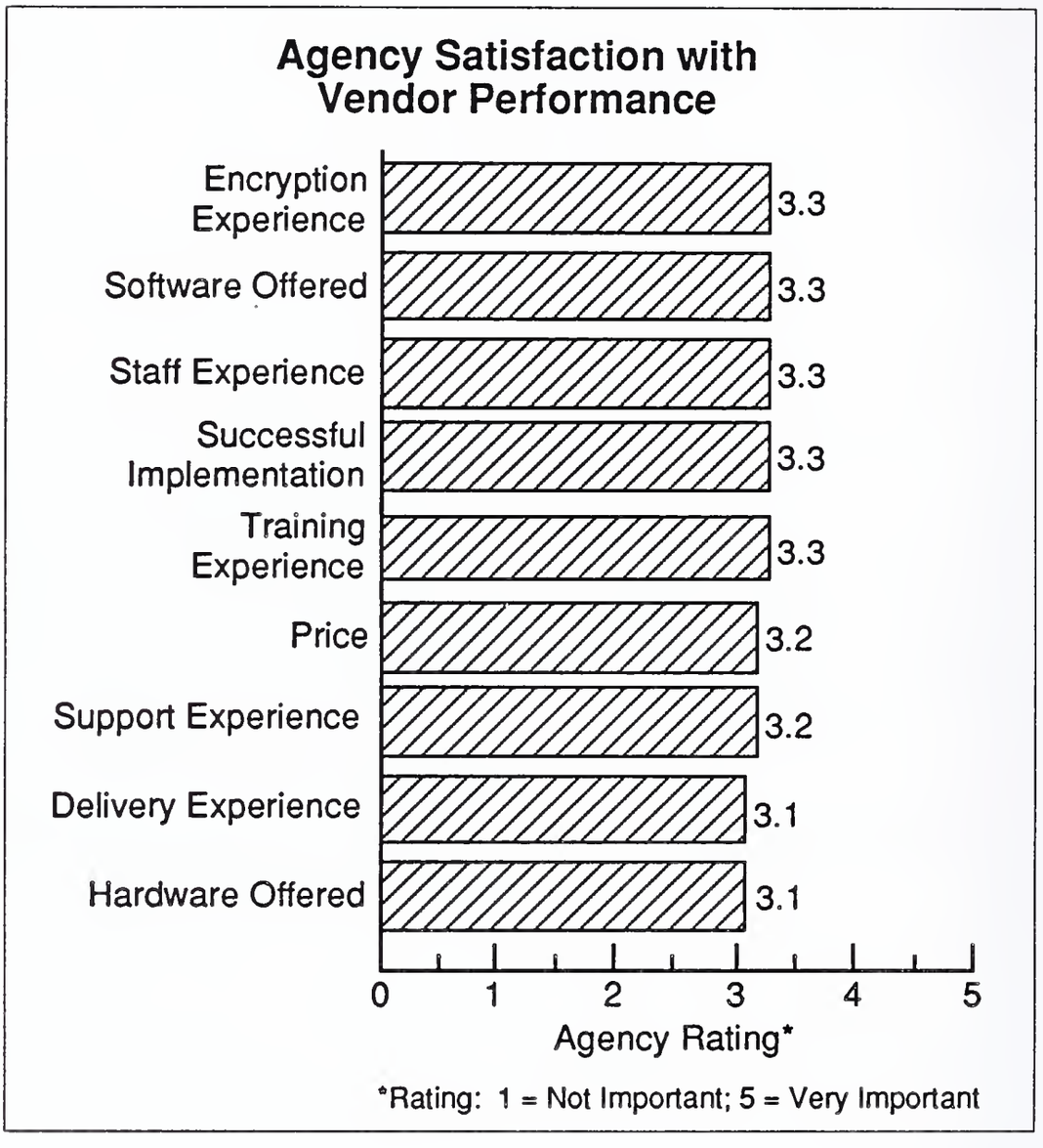
G

Vendor Performance

1. Agency Satisfaction with Vendor Performance

The overall level of satisfaction of agency respondents to vendor performance characteristics is moderate for all factors. Exhibit IV-16 displays the ratings given to each factor. Note that there are relatively few differences among the factors regarding vendor experience and product performance, all receiving ratings in the 3.1 to 3.3 range. This moderate rating improved, however, as vendors became more familiar with agency security requirements that are unique to their missions or agency operations of sensitive systems.

EXHIBIT IV-16



2. Preference for Type of Vendor

Agency respondents were asked which type of vendor is preferable for providing appropriate computer security products and services for their agency, as shown in Exhibit IV-17. Sixty-five percent of the agencies preferred software vendors, and stated that these vendors are responsive to meeting a variety of agency security requirements with their products, and also provide product support as needed.

The next largest share (50%) of the respondents preferred hardware vendors and professional services firms due to their flexibility in providing the agency with various options and services. At present, most agencies do not view systems integrators as the most appropriate vendors for the installation of computer security products/services. However, as security requirements and features are installed on more networks and

systems, the use of systems integrators may increase in the future. Systems integrators wishing to penetrate this area must augment their marketing efforts.

EXHIBIT IV-17

Agency Views on Appropriate Vendors for Computer Security Products/Services

Type of Vendors	Percent of Respondents*
Software Vendors	65
Hardware Vendors	50
Professional Services Firms	50
Systems Integrators	30
Aerospace Divisions	5
Not-for-Profit Firms	5

*Total exceeds 100% due to multiple responses.

3. Agency Suggestions for Improvements to Vendor Products and Services

Agency respondents were asked for suggestions on how vendors might make their computer security products and services more valuable to the federal government over the next five years. Exhibit IV-18 lists the principal suggestions made by the agencies. As should be expected, the replies varied due to the different types and levels of experiences the respondents have encountered with vendors. No ranking is available because of the diversity of replies from respondents.

The agencies are looking to future products to increase user education and security awareness. This is tied to the mandated requirements for employee training at federal agencies. The respondents also continue to stress the need for software-related security, both at application and system software level.

Also mentioned were suggested improvements to the focus of the vendor's offerings to more of a government orientation. Apparently, respondents are expressing dissatisfaction with modified commercial

offerings and need security products specifically geared to the government's mission and application areas. Furthermore, the products need to be available and delivered in a more timely manner.

EXHIBIT IV-18

Suggested Improvements to Security Products and Services

- Increase user education/awareness of security
- Integrate security into application and system software
- Increase government orientation
- Improve availability/delivery schedules
- Improve ease of implementation
- Stress security at development phase (avoid retrofit)
- Increase UNIX-based security products

As noted in other INPUT federal market studies, the agencies again suggested improvements to implementation. This shows that implementation of security products, along with other areas of software and hardware, still remains an issue with many respondents. Perhaps another suggestion made by respondents—to stress security at the system development phase—would eliminate some implementation problems. In addition, early incorporation of security features would avoid the costs and inefficiencies associated with retrofitting systems with security measures at a later stage. The solution lies with both the agencies in stating requirements and the vendors in providing for these measures.

Although not cited by the majority of respondents, a small group of respondents suggested that vendors increase their UNIX-based products. UNIX products in general are still developing and gaining a foothold in the federal market. The demand for UNIX-based security products may increase UNIX popularity and exposure in the federal environment.

H

Trends

1. Technology Trends

Agency representatives were asked to identify technological factors that could affect their agency's computer security requirements through FY 1993. Numerous factors were identified and those mentioned most frequently are listed in Exhibit IV-19.

EXHIBIT IV-19

Technological Trends Affecting Computer Security

Trend/Factor	Rank*
Expanded Networks/LANs	1
Intersystem Compatibility/OSI	2
Increased Use of Microcomputers	3
Advancements in Security Devices/ Safeguards	4
Developments in Telecommunications	5
Image Processing Technology	6

*Rank based on frequency of mention by respondents.

Many respondents identified expanded networks (especially local-area networks) and distributed processing network availability as important technological factors impacting their agencies' security requirements. The additional and more complex networks could increase access control problems and system vulnerability. OSI security is also causing some concern. Although the Government Open Systems Interconnection Profile (GOSIP) has gone into effect, security problems have not been resolved. It is widely believed that OSI security has been delayed by a lack of standards. Since GOSIP emphasizes ease of access, it creates an opportunity for security violations.

Intersystem compatibility and implementation of OSI, though contributing to the flexibility and adaptability of governmental information systems, also amplify most of the existing computer security problems and possibly pose new ones. Agencies need to be able to achieve greater productivity via OSI over the next few years and still protect their sensitive data.

The respondents also mentioned increased use of microcomputers as a significant factor affecting future computer security requirements. As noted earlier, microcomputers already pose serious security problems which will be compounded with the increase in the number of users. It is difficult to enforce security regulations on users of microcomputers. Furthermore, the computers are geographically dispersed among different user groups and applications, therefore more accessible and subject to unauthorized and possibly infected software.

On the positive side, the agencies did see future technologies bringing about advances in computer security devices to better serve the growing demand for products. Examples of enhancements to system safeguards included improved encryption techniques, software logging procedures, and secure optical disks.

Telecommunications developments such as fiber optics will impact the security requirements and products sought by agencies. The introduction of supplemental methods of communicating between systems or accessing a network will serve to compound the security features needed for systems.

Image technology allows users to electronically store, process, and retrieve information, including text and graphics on a computer. As this technology and related products become widely available, managing the security efficiently and still achieving productivity and savings gains will be a challenge for the 1990s.

Agency respondents also gave their views on the impact that the technological advances mentioned will have on computer security requirements and computer operations. Respondents clearly perceive greater difficulties in the future for controlling system accessibility and protecting data integrity arising from advanced technologies. They also expressed their concerns for ease of implementation. In addition, some agencies foresee a favorable influence as the new technologies will increase the flexibility of system security and allow for more appropriate tools to be designed. Lastly, the respondents are hopeful that the increases in LANs and networks will eventually lead to development of specialized safeguards for networks.

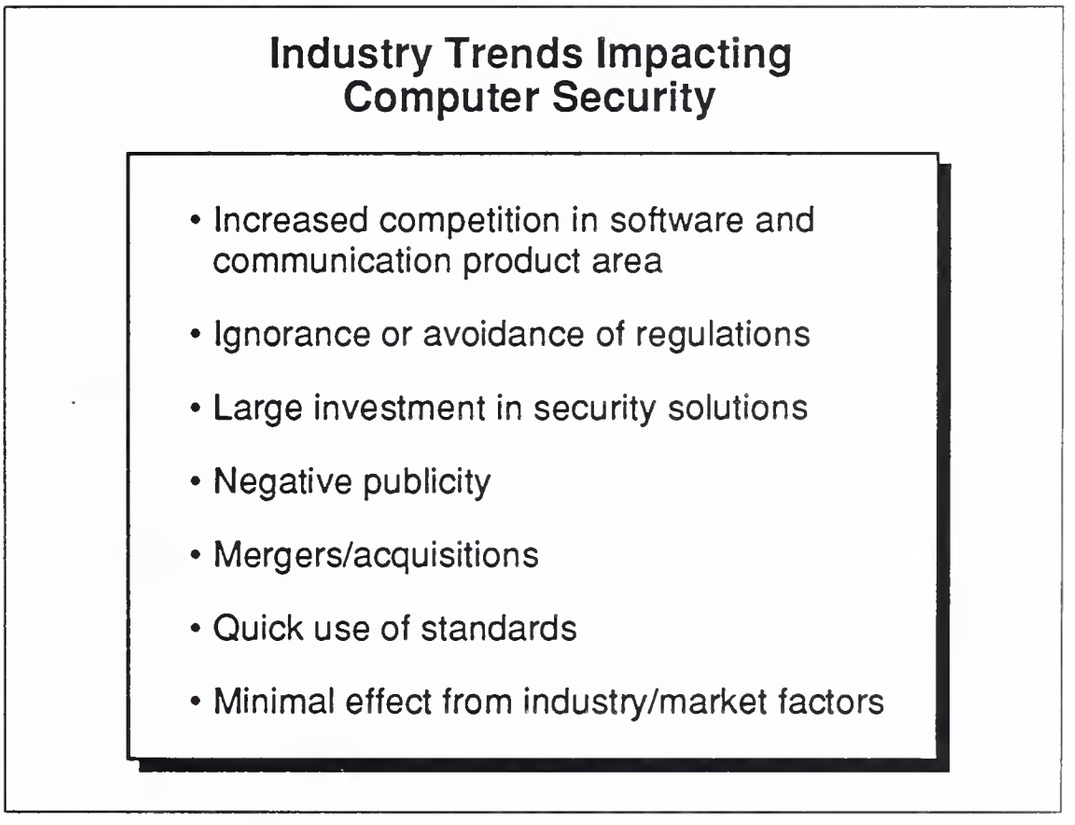
NIST has taken a somewhat unusual approach in assessing the impact of technology trends. In 1988, NIST established the Risk Management Research Laboratory to advance leading-edge technology in assessing and managing computer-associated risks. Initially, the lab evaluated two dozen risk assessment packages. These packages were then used for constructing a conceptual framework for risk management. The lab will now assemble risk scenarios and evaluate the effectiveness of the framework.

2. Industry Trends

The agency respondents were asked to identify industry trends and nontechnical factors that could significantly impact the agency's computer security plans. Exhibit IV-20 summarizes the agency responses. There is no ranking due to the diversity of responses.

Many of the respondents mentioned increased competition for software and communications products. Several companies, which traditionally are in the federal software and communications market, have expanded into computer security products. Other sources of competition are commercial sector computer security firms which are now targeting the federal market, along with start-up federally-oriented security companies.

EXHIBIT IV-20



Mergers and acquisitions in the industry will continue during the 1990s. In some cases, depending on the product/service offered, a large investment of capital may be required to develop and provide the security solutions geared to the government's mission and applications. Vendors with a strong financial background and good management skills will be best suited to survive the financial risks involved with the market.

The respondents expressed views on both sides of the compliance issue. Some indicated that vendors ignore or avoid regulations, while others noted quick adherence to standards. Since federal agencies are required to adhere to specific standards and regulations, companies that offer products that comply are expected to gain a stronger foothold at the agencies.

Publicity regarding computer viruses and other attacks on the security of government computer systems will also impact the federal computer security market. Agency respondents are concerned that too much notoriety will spur other acts of computer vandalism. Also, negative publicity tends to increase Congressional and public inquiries into security operations, further complicating computer plans and requirements.

3. Budgetary Constraints

The majority of the agencies surveyed said that they experienced budgetary constraints attributable to the Gramm-Rudman-Hollings Act or other federal government budgetary constraints. Exhibit IV-21 shows the variety of impacts resulting from budgetary cuts on the development and implementation of computer security plans at the respondents' agencies.

EXHIBIT IV-21

Impact of Budgetary Constraints

Impact	Rank*
"Devastating Effect"	1
Cuts Security Awareness and Training Programs	2
Limited Impact/Restricts Flexibility	3
Difficult to Fund Planned/Additional Programs	4
Limits Staffing Levels	5
Delays Network Encryption	6

*Rank based on frequency of mention by respondents.

The most frequently mentioned impact was that budgetary constraints have a "devastating" or highly significant effect. This implies that implementation has been seriously hindered or cancelled by lack of funding. Specifically targeted cuts have occurred in agency security awareness and training programs.

Some agencies have suffered major delays and cutbacks in acquisitions, and other agencies have downsized levels of support and slowed their implementation efforts. Several agencies commented that at present they have encountered a minimal amount of budgetary constraint, but foresee more significant funding restrictions in the future.

4. Impact of Government Policy Agencies

Computer security for federal information systems is subject to a range of governmental policies, regulations, and other influences from policy-formulating agencies. Therefore, the agency respondents were surveyed to obtain their views on how several government regulations and policies from selected agencies would impact their agency's computer security requirements and acquisitions through FY 1993. Exhibit IV-22 shows each agency studied, and the general responses of agency officials. (A previous discussion of security regulations and policies was included in Section III.)

EXHIBIT IV-22

Respondent Views on Impact of Government Policies

- NIST
  - Set standards/guidelines to follow
  - Compliance may require increased training and security reviews
  - Manage relevant FIPS
  - NIST efforts benefit agencies
- NSA
  - Provide helpful assistance
  - Greatly impact COMSEC environment
  - Provide review and certification for products
  - Publish guidelines for encryption
  - Directly impact classified data systems
- GSA
  - Minimal/little impact
  - Improve contract methods
  - Publish security regulations
  - Uncertain of impact of FTS 2000

In general, respondents viewed the activities and security guidelines provided by NIST and NSA as beneficial. In complying with the standards and guidelines set, some respondents noted the possibility of having to increase their training and security reviews. The majority of respondents view GSA as having minimal impact on the federal computer security market.

NSA's area of impact is more apparent in the product evaluation/certification process and the COMSEC environment. NSA product approval is highly sought by many vendors. The agency also has a strong role in establishing security procedures for classified data systems.

Respondents also commented that they expect GAO and agency Inspector General internal audits to increase reviews and oversight in the security area. In addition, it was expected that OFPP will be more active in establishing overall government strategies. Agency officials further anticipate that future legislation will required additional procedures to be implemented. This may result in the need for additional consulting services and installation of new tools.

The NSA has initiated two programs to foster the development of secure communications equipment for both classified and unclassified applications. The programs are referred to as Project Overtake and the Commercial COMSEC Endorsement Program (CCEP). The following vendors are participating in Project Overtake:

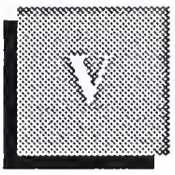
- AT&T
- GTE
- Harris
- Honeywell
- Hughes
- IBM
- Intel
- Motorola
- RCA
- Rockwell

Through Project Overtake, vendors are reducing the size and cost of encryption modules and embedding them in computer and communications equipment.

NIST is also having an impact in still another way. It has established a governmentwide information network on security issues. NIST is organizing agency security incident response and resource centers into a network that will:

- Supply the latest information on security threats
- Develop a program to report and assess security incidents
- Offer assistance

Several agencies are working with NIST on the project, including Energy, Justice, Transportation, NASA, and the National Science Foundation.



Competitive Trends

This section presents the results of the vendor surveys and other competitive information.

Vendors responding to this survey provide a wide range of products and services to the federal computer security market. They also generate different levels of revenue. However, very few derive a large portion of their revenue from federal computer security. This suggests that security is an ancillary activity for most firms.

Although the vendors favored Defense agencies for security sales opportunities, Treasury ranked first in terms of agency opportunities. This suggests that many vendors recognize the special security concerns at Treasury and intend to participate in Treasury business.

In general, vendors expect their computer security revenues to increase. They view the market as better defined than do agency respondents. However, they do show concern for the complexity of requirements and the relative lack of standards.

A Vendor Participation

1. Vendor Products and Services

Exhibit V-1 shows the products and services that the vendors surveyed indicated they sold to federal agencies. Presently, the vendors' offerings emphasize secure network products, communications security, and software-driven password security. These are some of the same product areas that the agencies indicated earlier in Exhibit IV-13 that they would be acquiring through 1993.

Some of the vendors interviewed are new entrants to the market and their responses covered planned products. The majority of industry respondents also noted that they plan to provide additional security products and services in the future in response to demands from government clients.

EXHIBIT V-1

Products and Services Provided to Federal Agencies

Products/Services	Percent of Respondents*
Secure Networking Products	64
Communications Security Products	57
Software-Driven Password Security	57
Data Encryption Equipment	54
Contractor Assistance for Preparation of Plans	50
Other Contractor Support	50
Secure UNIX-based Products	46
Secure Workstations	43
Risk Management Analysis	32
Other Computer Security Devices	32
Tempest Products	29
Emission Control Devices	21
Security Training Tools	21

*Total exceeds 100% due to multiple responses.

2. Vendor Respondent Revenue Characteristics

Exhibit V-2 displays a profile of vendor respondents from the perspective of total corporate revenues for FY 1988. The data was developed solely from the survey efforts. The vendor respondents represented many of the largest hardware and software suppliers to the industry as a whole and to the federal government sector. Also included are some of the specialized computer security firms. As shown in the exhibit, there was

no particular pattern in revenue size. Rather, respondents spanned a wide range of sizes, as well as activities.

EXHIBIT V-2

Vendor Respondents' FY 1988 Revenues

Revenue	Percent of Respondents*
Under $50 Million	11
$50 to $100 Million	16
$100 to $500 Million	11
$500 Million to $1 Billion	0
$1 to $5 Billion	32
$5 to $10 Billion	21
$10 to $20 Billion	11

*Total may exceed 100% due to rounding.

The distribution of the surveyed companies' revenues derived from the federal computer security market is shown in Exhibit V-3. The largest share (41%) of respondents obtain approximately 1% of their revenues from this market. However, most vendors are optimistic about increasing this segment of their federal business. For none of those surveyed did federal computer security business represent a majority of revenue.

EXHIBIT V-3

Current Percent of Vendor Revenue Derived from Federal Security Market

Percent Revenue	Percent of Respondents*
0	12
1	41
2 to 5	6
5 to 10	18
10 to 20	12
20 to 80	0
80 to 90	6
90 to 100	6

*Total may not equal 100% due to rounding.

3. Industry Leaders in the Federal Computer Security Market

A ranking of the leading vendors in the federal computer security market, based on the frequency of mention by industry respondents, is provided in Exhibit V-4. For the most part, these companies have demonstrated the capabilities to comply with security standards and incorporate security processes and technology into their products and services. These help to satisfy the federal agencies' needs for end-user computer and networking security.

The companies mentioned most frequently—such as Digital, AT&T, and IBM—are moving into the security market through existing hardware product lines and supporting products in order to retain their foothold in the federal marketplace. Furthermore, many of the companies listed in Exhibit V-4 are also leading suppliers to defense agencies and thus gear their products to comply with the security standards essential to defense computer systems. Other companies mentioned are becoming well-known for their workstation products, which are being modified to incorporate government-required security features.

EXHIBIT V-4

Leading Federal Security Vendors in Vendor Perspective

Vendors	Rank*
Digital Equipment Corporation	1
AT&T	2
IBM	3
Honeywell	4
Motorola	5
TRW	5
Xerox	6
Computer Associates	6
Unisys	6
Boeing Computer Services	7
Sun Microsystems Inc.	7
Trusted Information Systems	7

*Rank based on frequency of mention by industry respondents.

It is interesting to note that the top five vendors in the list are principally associated with computer equipment. This suggests a perception on the part of the vendor community that computer security is focused on hardware.

B
Vendor Market Perceptions

1. Federal Agency Opportunities

The majority of the industry respondents provide their products and services to both the DoD and civilian agencies. INPUT asked which agencies can be identified as the best opportunities for a given company in the computer security market. The major defense agencies and NSA, along with several large civilian agencies such as Treasury, Energy and

Justice were mentioned most frequently, as shown in Exhibit V-5. Besides the civilian agencies listed, other agencies listed by the respondents include Transportation, HHS, Agriculture and Commerce.

EXHIBIT V-5

Leading Agency Opportunities for Security Products and Services

Federal Agency	Rank*
Treasury	1
Air Force	2
National Security Agency	3
Navy	4
Army	5
Defense Intelligence Agency	6
Defense Communications Agency	7
Central Intelligence Agency	8
Energy	9
Justice	10
NASA	11
Defense Logistics Agency	12

*Rank based on frequency of mention by industry respondents.

For many vendors, the defense agencies are long-term targets for their products and services, since they are already well-known at these agencies. The civilian agencies are considered a growing market segment, in view of additional security requirements the agencies are adding to comply with government legislation. Additional technological advances and product availability will fuel both of these market segments.

2. Differences Between Defense and Civilian Agency Markets

Exhibit V-6 presents the industry respondents' opinions on the differences between the defense and civilian agency markets for computer security products and services. The majority of respondents noted that more numerous and stricter requirements and standards are imposed upon the defense agencies than on the civilian agencies.

EXHIBIT V-6

Agency Security Market Differences

Defense Market	Civilian Market	Rank*
More Stringent Requirements and Standards	Fewer Mandated Requirements and Standards	1
Greater Security Awareness and Experience	Less Awareness/Greater Need for Training	2
Larger Volume of Classified Data/Greater Concern for National Security	Less Classified Data/Concern for Authentication and Integrity of Sensitive Data	3
Closer Adherence to Software Development Standards and Customized Systems	More Reliance on Hardware Only/Reluctant to Invest in Software Due to Cost	4
Require Military-Grade Encryption and Higher Levels of Security	Can Utilize DES-Based Encryption and Lower Level of Security	5

*Rank based on frequency of mention by respondents.

The second most notable difference was the greater level of security awareness at defense agencies and a more experienced staff. At the civilian agencies there is a greater need for training to bring them up to the level of awareness required by the Computer Security Act. This training is already underway at most agencies.

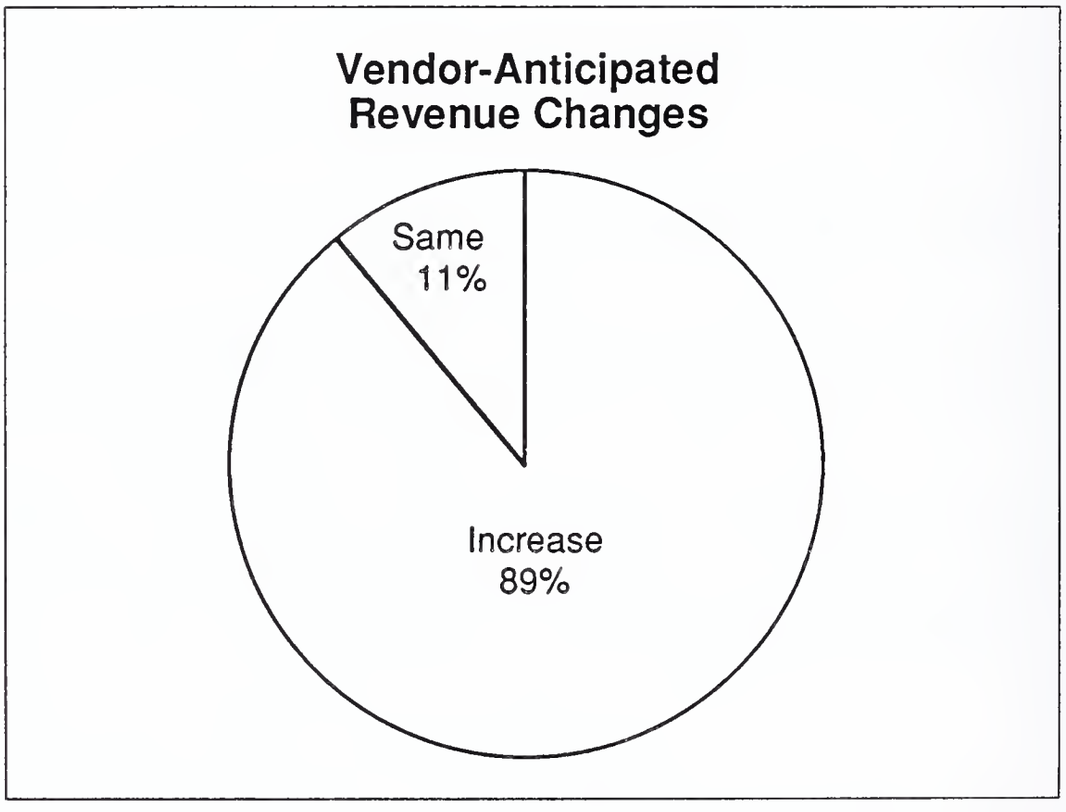
The mission of the defense agencies results in a larger volume of classified data and higher imposed levels of security. The classified systems and the concern for national security also result in an increased potential at some defense agencies for customized security systems and software.

Currently, the civilian agencies are focusing on hardware-based security solutions and are not as willing to invest as much as the DoD is to acquire software for computer security implementation. Since their volume of classified data is much lower, most civilian agencies are able to utilize lower levels of security to protect the authenticity and integrity of their data. However, communications security is becoming very important in some civilian agency processes, such as those dealing with cash management and electronic funds transfer.

3. Anticipated Increases/Decreases in the Federal Computer Security Market

Most of the vendors surveyed expect their revenues from the federal computer security market to increase over the next five years, as illustrated in Exhibit V-7. None of the respondents forecasted a revenue decrease, and only eleven percent believed that revenues will remain at their present levels.

EXHIBIT V-7



Vendors also anticipate increases in their market share as a result of six main factors. Exhibit V-8 shows that many respondents (29%) expect their revenues to increase as the government increases its security requirements. Technological improvements and implementation of additional standards will also cause revenues to rise as the market expands and new products are made available. Several respondents are new to this market, and consequently have only a small market share. New vendors expect their revenues to increase as they participate in more—and possi-

expect their revenues to increase as they participate in more—and possibly larger—procurements.

EXHIBIT V-8

Reasons for Vendor Revenue Increase FY 1990-FY 1994

Reason	Percent of Respondents*
Increased Security Requirements	29
New Products Available	25
Expanding Market	25
Increased Government Demand	18
New in Market	7
Increased Security Awareness	7

*Total greater than 100% due to multiple responses.

Those vendors who believe that the federal computer security market will be leveling off through 1993 indicated that the budgetary cutbacks, the lengthy certification process, and market penetration would be the key forces holding down growth. Potential limits to funding and a more competitive arena could pose strong threats to the well-known vendors in this market.

INPUT forecasts that the federal computer security market will grow at a compound annual growth rate of 4% through 1995. Exhibit V-9 presents the market growth rates estimated by the industry respondents. The largest number of responses were in the 10 to 15% and 20 to 25% growth ranges. Overall, there was a high level of optimism among some respondents, with 15% of those surveyed estimating growth of 50% or more for the forecast period. The future of the federal sector of this marketplace is viewed more positively than the future of the security industry in general.

EXHIBIT V-9

Estimated Market Growth through 1994

Percent Estimated Growth	Percent of Respondents
Under 10	11
10 to 15	26
15 to 20	7
20 to 25	22
25 to 30	7
30 to 50	11
50 and up	15

*Total may not equal 100% due to rounding.

4. Advantages to the Federal Computer Security Market

Vendors surveyed by INPUT had wide-ranging opinions on the advantages of competing in the federal computer security market. Their responses are summarized in Exhibit V-10.

The industry respondents noted their ability to build on their previous computer security experience and recognition in the industry. This enables them to penetrate the federal market more quickly than some other market segments. Their early successes also reveal more opportunities within the government. They believe that the federal security market has the benefit of already having established requirements and standards with which the vendors must comply, rather than being in the midst of evolving standards.

Computer security at federal agencies entails some large-scale procurements with sizeable dollar values that attract vendors to the federal marketplace. Parts of the civilian sector could become a volume-oriented market, creating multiple opportunities due to the similarity of hardware and software solutions that can be used in a variety of applications. Vendors also noted that the federal market is a precursor to the

commercial market, and early developmental efforts are financially rewarded with the future demand for commercial off-the-shelf products.

EXHIBIT V-10

Advantages in the Federal Computer Security Market

Advantage	Rank*
Leveraging Experience and Industry Reputation	1
Well-defined Requirements in Most Areas	2
Meaningful Standards already Established and Being Adopted	3
Size of Contracts (large)	4
Development and Demand for Commercial Off-the-Shelf Products	5

*Rank based on frequency of mention by industry repondents.

5. Problems in the Federal Computer Security Market

Vendor views of the problems or disadvantages associated with this segment of the federal marketplace also span a wide range, as shown in Exhibit V-11. The most frequently mentioned problem is the necessity of complying with complex requirements and standards. Vendors expressed their frustration in trying to supply products that are compliant with highly technical and rigid standards.

Federal budgetary constraints pose a problem to vendors as agencies are not allocating significant funding for the implementation of computer security. The agencies are mindful of the need to avoid expensive retrofitting of systems, but have not yet made a full-fledged effort to build in security as systems are developing.

EXHIBIT V-11

Problems Associated with Federal Computer Security Market

Problem	Rank*
Complexity of Requirements/Standards	1
Lack of Funding/Low Budgets	2
Lack of Awareness/Educated Users	3
Lengthy Product Certification Process	4
Lengthy Procurement Process/Threats of Protests	5

*Rank based on frequency of mention by industry respondents.

Presently, industry respondents are facing the problem of dealing with users who are lacking in security awareness and training. This hampers the demand for security products as well as making implementation more difficult. The required level of sensitivity does not yet exist in many agencies. Although some marketing will help, budget constraints will continue to dampen market growth.

Vendors are burdened by both a tedious and lengthy product certification process and the federal procurement process. These long procedures prevent companies from bringing products to the market in a timely manner. They can also cut into the potential for company profits.

Other concerns mentioned by vendors were:

- User acceptance/compliance
- Obtaining clearances
- Increased competition
- Lack of qualified personnel for implementation
- Limited enforcement of regulations

The NCSC's Evaluated Products List (EPL) is also judged inadequate by some vendors. One vendor official, William Norvell of Hughes, was quoted as saying that secure systems often fail "not because they do not meet regulations, but because they fail to meet unspecified operational requirements."

C

Vendor Contracting Views

1. Preferred Contractors

Vendors were asked to indicate which type of company they believe federal agencies will prefer, in rank order of preference. As illustrated in Exhibit V-12, industry respondents believe that the use of systems integrators is most preferable to the agencies. Many vendors are currently offering or planning to offer systems integration services.

EXHIBIT V-12

Vendor Perceptions of Agency Preferences for Security Contractors

Type of Contractor	Vendor Rank*
Systems Integrator	1
Hardware Vendor	2
Software Manufacturers	3
Professional Services Firm	4
Aerospace Divisions	5
Not-for-Profit	6
Foreign Manufacturers	7

*Rank based on average score for each contractor type.

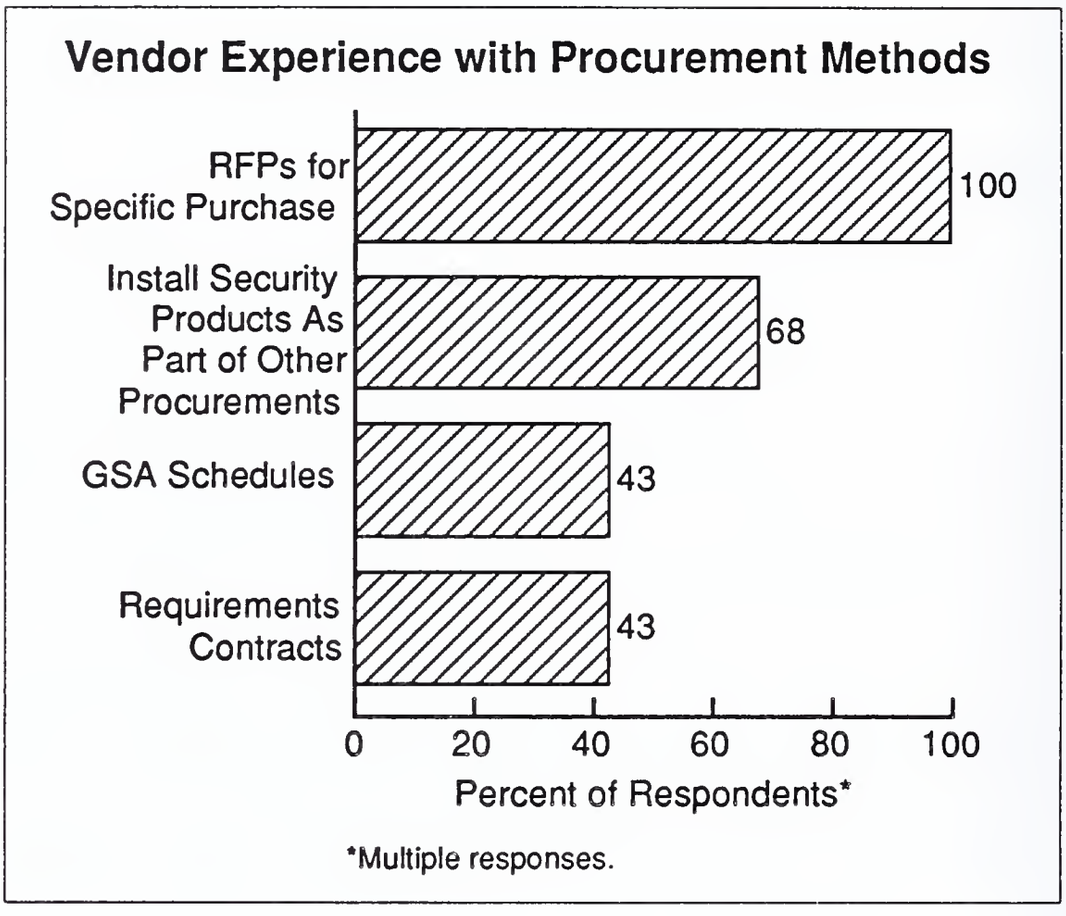
Vendors also believe that agencies prefer to use the services of hardware and software companies to undertake implementation of security programs. These vendors appear to be a logical choice, since they can supply the right match of skills and resources required for many federal projects and are already strong players in the market. There was no indication of agency preferences for 8(a) and other minority businesses.

2. Vendor Experience with Procurement Methods

Vendors were queried about which procurement methods they have responded to in marketing their computer security products and services to the federal government. Results are shown in Exhibit V-13. All of the industry representatives surveyed have responded to RFPs from agencies. Over two-thirds of the respondents have installed security products and services as part of other procurements. A smaller share of vendors (43%) currently participate on the GSA Schedules. This method of

providing products to the government is likely to increase over the next two to five years. At present, there are very few requirements contracts for computer security products and services.

EXHIBIT V-13



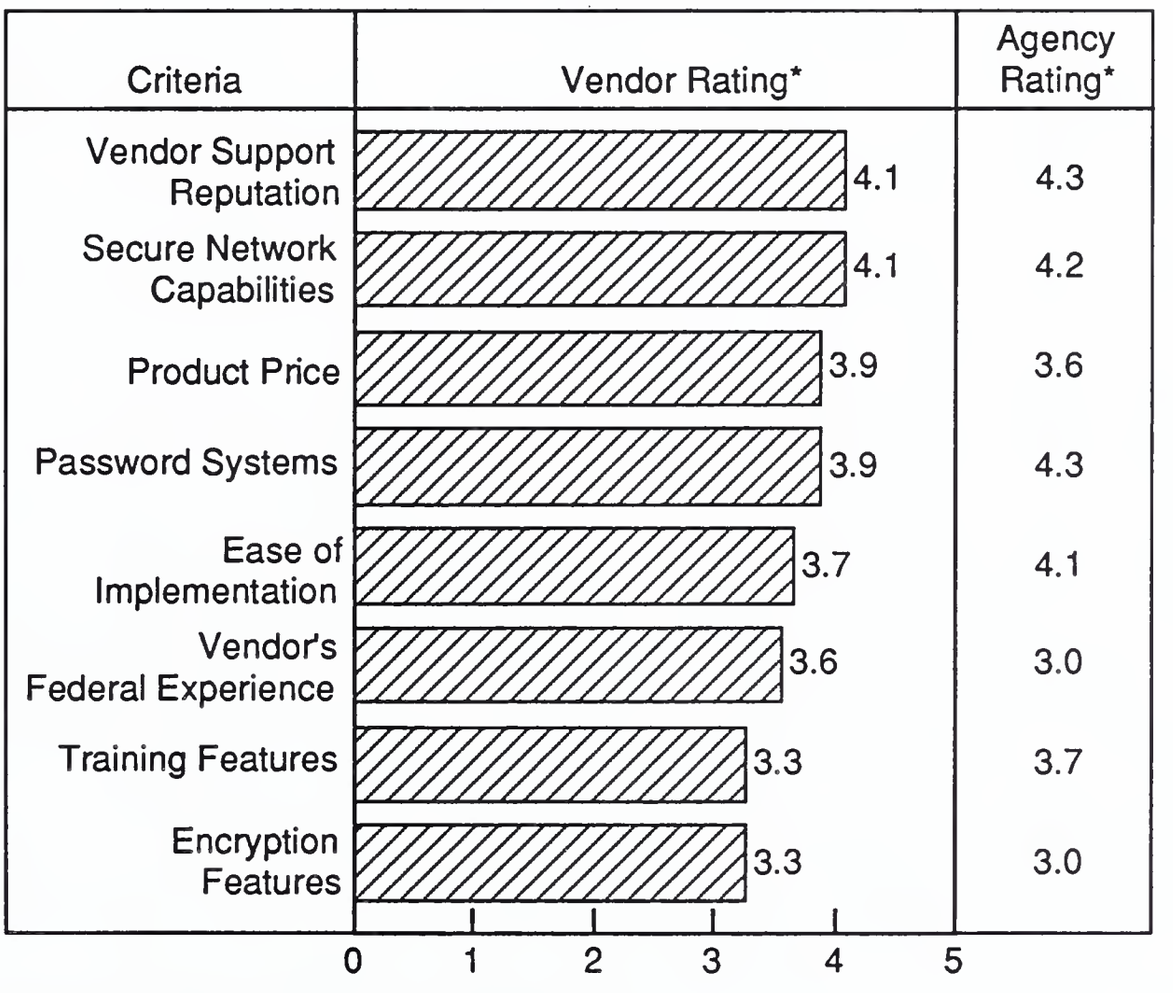
3. Vendor Selection Criteria

Vendors need to better understand and respond to the criteria utilized by the government in selecting a winning vendor for computer security products and services. As shown in Exhibit V-14, industry respondents consider the vendor's support reputation the number-one selection criterion. This suggests the importance of service in meeting federal security needs. The agencies concur with the vendor perceptions. The two respondent groups also gave similarly high ratings for the importance of secure network capabilities.

The agencies indicated greater importance of password systems, ease of implementation, and training features than did the industry vendors. This may arise from agencies having a user perspective. The industry respondents placed more importance on federal experience than was apparant to the agencies. However, both groups are in some agreement on the moderate range of importance for product price and encryption features.

EXHIBIT V-14

Vendor Selection Criteria



*Rating: 1 = not important, 5 = very important.

D

Teaming Patterns

Teaming efforts in the federal market are becoming more frequent in order to respond to the terms and conditions of many agency RFPs. Most vendors view their teaming relationships as moderately successful, with the average rating at 3.7. This suggests that vendors may need to improve their teaming efforts.

Exhibit V-15 lists the respondents' rating of their levels of success. Over one-third (36%) selected a rating level of three, indicating moderate success. Another 20% each indicated a rating of either 4 or 5, which suggests a considerably high degree of satisfaction with their current teaming experiences.

EXHIBIT V-15

Success Level of Vendor Teaming Relationships

Success Level*	Percent of Respondents
1	0
2	4
3	36
4	20
5	20
No Response/ No Teaming Experience	20

Note: Overall teaming success rating: 3.7, based on a 1 to 5 scale.

*1 = not successful at all, 5 = extremely successful.

Exhibit V-16 lists vendor types cited by the industry respondents as their most frequent teaming partners. Software and hardware vendors combined are mentioned most often as team members. They are chosen for their ability to provide the appropriate skills and resources required for many federal projects and their understanding of the existing computer systems.

A close second place for mention as partners were systems integrators. As noted earlier, many of the companies surveyed are already performing systems integration functions or will be in the future. Also, in the next few years, teaming with the Tempest hardware firms and small market niche companies may increase as security requirements to be implemented call upon the specialized expertise of these companies.

Teaming activities present their own set of related vendor concerns and issues. In previous INPUT studies of teaming among vendors, the industry respondents recognized the need for more cooperation and communication with its teaming partners. The vendors also noted their own shortcomings in not fully identifying all the requirements of a program early enough in the planning process. If overcome by computer security

vendors, this better planning could aid in developing stronger teaming of companies that are more suitably matched.

EXHIBIT V-16

Preferred Teaming Partner for Security Contracts

Vendor Type	Percent of Respondents
Hardware and Software Vendors	27
Systems Integrators	23
Hardware Manufacturers and Systems Integrators	14
Hardware Manufacturers and Professional Services Firms	9
Software Firms	9
Tempest Hardware Firms	9
Small Market Niche Companies	9

Industry respondents have also mentioned in previous studies the need to improve the marketing of their team members' products as well as increasing their reliance on standard products. In addition, teaming efforts should focus on improving delivery schedules and product prices. These suggestions appear relevant to the federal computer security market.

E
Vendor Performance

1. Ratings for Vendor Performance

Both agency and vendor respondents were asked to evaluate agency perceptions of vendor performance characteristics. Exhibit V-17 compares the vendors' and agencies' ratings of these characteristics.

Some differences in opinion appear to exist between the two respondent groups. The characteristic rated most satisfactory by the vendors was hardware offered, whereas the agencies experienced lower levels of satisfaction from the products acquired.

EXHIBIT V-17

Comparative Ratings of Vendor Performance

Characteristic	Vendor Rating*	Agency Rating*
Hardware Offered	3.5	3.1
Encryption Experience	3.4	3.3
Successful Implementation	3.3	3.3
Training Experience	3.1	3.3
Staff Experience	3.1	3.3
Software Offered	3.0	3.3
Price	3.0	3.2
Support Experience	3.0	3.2
Delivery Schedule	2.7	3.1

*Rating: 1 = definitely not satisfactory, 5 = outstanding performance.

There are minor differences between the responses from the agencies and vendors on most other characteristics. However, for their adherence to delivery schedules, the industry respondents rated industry performance at only 2.7, while agencies averaged a 3.1 rating for this characteristic. This suggests that vendors are already aware of their need to improve timely availability of products in line with the agencies' perceptions of successful vendors.

2. Suggested Improvements to Products and Services

Industry respondents were asked what improvements vendors could make to their products and services over the next five years to make them more valuable to the federal market. Exhibit V-18 lists the responses.

The replies varied as a result of different types and levels of experience vendors have encountered with federal agencies. Improvements to the user friendliness of security products and services were mentioned by the largest percentage of the respondents. This improvement, along with the increased awareness and training of federal personnel/users, could help to promote more effective use of security safeguards.

EXHIBIT V-18

Suggested Improvements for Security Products and Services

Suggestion	Percent of Respondents
Improve User Friendliness	21
Offer a Broad Range of Interoperable Systems	18
Improve Software Security Features	18
Other	14
Lower the Price	11
Standardize Security on Off-the-Shelf Technology	11
Shorten Cycle of Validation/Certification	7

The suggested improvements to interoperability of systems and improved software features are similar to suggestions made by the agency respondents. Some vendors noted that standardizing with off-the-shelf technology would improve their business relationships with the federal government as agencies are seeking cost-effective solutions to security requirements.

Only a few vendors acknowledged possible improvements to the lengthy validation and certification processes. These processes are essential to the development of products in order to comply with a full range of rigid requirements and standards.

Other suggestions made by the industry respondents include:

- Improved training
- Development of nonproprietary architecture
- Improved compliance with federal market demand
- Improved accuracy in advertisements of product capabilities

F
Trends

1. Technology Trends

Industry representatives were asked to identify technological factors that would affect the federal government's computer security requirements. The factors named most frequently are listed in Exhibit V-19.

EXHIBIT V-19

Vendor Ranking of Technological Factors Affecting Computer Security

Factor	Vendor Rank*
Increase in Networking Capabilities	1
Developments in Workstation Environment	2
Increase in Distributed Processing	3
Advancements and Increased Use of RDBMS	4
Standardization Efforts	4
Migration of Open Systems	4
Advancements in Hardware to Incorporate Security Features	5
Implementation of UNIX/POSIX	5
Developments in Telecommunications	6

*Rank based on frequency of mention by respondents.

The vendors frequently noted that additional and more complex networking capabilities will increase the computer system access control requirements and also require the development of security safeguards for information storage and transmission. Agency respondents selected expanded networks as the top-ranked technological factor to affect the federal computer market over the next few years.

The increased use of workstations at agencies for end-user computing has necessitated that industry bring secure technology down to the workstation level. Products such as SecureWare's Compartmented Mode Workstation (CMW) and Contel's Secure Workstations Project already

show the efforts of some firms to move into this segment of the federal marketplace. Contel is installing 1,200 high-end Sun Microsystems at OSD, under a project called the Office Automation Secure Information System (OASIS). Further, under its Compartmented Mode Workstation procurement, the DIA is buying secure workstations from Harris, Digital, and IBM.

Distributed processing is also contributing to agencies increasing their security requirements. The development of programmable intelligence in order to perform data processing functions more effectively through computers and terminals arranged in a telecommunications network will result in a greater agency need for encryption of data transmission lines.

As shown in Exhibit V-19, several technological factors tied for fourth place in frequency of mention. Many of the software vendors, as well as other companies surveyed, have noted that relational data base management systems (RDBMS) will impact the market. This market niche in general is already highly competitive.

Standardization efforts will continue to play a major role in the federal computer security market. In some cases, vendors are jointly working with federal organizations in developing standards that incorporate commercial developments and previous computer security expertise.

Intersystem compatibility and implementation of OSI will require that vendor security products contribute to the flexibility and adaptability of governmental information systems. Open systems will require security in various levels of the OSI model. The NIST Computer Systems Lab has been working with vendors to address the security issues of OSI.

Advances in hardware, implementation of UNIX/POSIX, and developments in telecommunications were technologies cited by both vendor and industry respondents as having an influence on federal computer security requirements and implementation. Many vendors are aware of the federal agencies' need to go beyond just physical and software security solutions, and are positioning themselves to offer the hardware to support agency applications in a secure environment in the future. POSIX will require application portability security, and along with UNIX is gaining a foothold governmentwide.

Telecommunications developments such as fiber optics will impact the security products to be developed by vendors. Additional methods of communicating between systems can extend the security features needed for the agency system. In general, any product or service which enhances interoperability also increases the need for security.

The NIST Technical Security Program plays an active role in the utilization of new technologies to enhance the security of federal computer

systems. NIST personnel are currently working on a variety of technical issues that will extend into the 1990s. These include:

- POSIX
- Network Security
- Data Encryption
- Key Management
- Message Authentication
- Network Access Control
- ISDN
- Anti-Virus Activities

NIST releases policy statements and technical publications in order to disseminate the technical information compiled by the various divisions of the National Computer Systems Laboratory.

2. Budgetary Constraints

As shown in Exhibit V-20, industry respondents expressed varying opinions as to the effects of federal budget constraints on the federal computer security market. The vendors view delays in implementation, funding cuts and downsizing of security efforts as the main effects. Twenty-one percent of the industry respondents viewed the effects as minimal due to the decreasing product price. However, many industry products are still considered costly by government agencies. As indicated in Chapter III, INPUT does not concur with this viewpoint. INPUT considers budget constraints to be the dominant negative market factor.

EXHIBIT V-20

Impact of Budgetary Constraints

Impact	Percent of Respondents
Delays Implementation of Security Features	25
Minimal Impact/Decreasing Product Prices	21
Security Low Priority/Cut from Budget	18
Other/No Response	18
Significant Impact	11
Downsize Security Efforts	7

Budget cuts will hinder the security training and implementation phases at many agencies, thus initially slowing market demand for some products and services. Furthermore, cancellation or reduced funding of a major systems procurement can result in a lengthy procurement process and potential loss of acquisitions for the security component of the proposed system.

3. Market Trends

The market factors that vendors believe will impact the federal computer security market were numerous and varied. INPUT listed the responses in order of frequency mentioned in Exhibit V-21.

EXHIBIT V-21

Market Trends Impacting Computer Security Market

Factor	Rank*
Availability of Security Products	1
Regulation/Computer Security Act	2
Mergers/Joint Ventures with Hardware and Software Firms	3
Privacy Issues	4

*Rank based on frequency of mention by respondents.

The marketplace is expected to change over the next two to five years as an influx of products become available. Additional UNIX-based products, secure workstations, and encryption systems will be competing for market share with existing products.

Federal regulations and the Computer Security Act will continue to provide guidance and direction to the industry. The proposed anti-virus legislation, fraud prevention, and other security-related agency directives give additional weight to the importance of computer security for federal information systems and may spark greater demand for products and services.

As in other segments of the information industry, the federal computer security marketplace is experiencing an increase in mergers and joint ventures. Economic conditions dictate that stronger competitors buy out

their weaker competition. Also smaller niche companies are targets of mergers/acquisitions by larger firms that are interested in more quickly marketing the specialized products. Joint ventures have become common between hardware and software firms in order to respond to more complex and all-inclusive government RFPs.

Many of the privacy issues related to computer security still remain unresolved. The government has information which, although nonclassified, is still only suitable for restrictive disclosure due to the protection of individuals' or corporations' rights to privacy. Legislation is pending that will reinforce privacy rights and inflict greater punishments for security violations.

4. Impact of Government Policy Agencies

Industry respondents were surveyed to obtain their views on how government policies and regulations from GSA, NIST, and NSA will impact the federal computer security market through FY 1993. The vendors gave a variety of responses that can be grouped into two general areas: the responsibilities of each specific agency studied, and the resulting impact on the federal computer security market. The following outline conveniently summarizes the comments received and supports INPUT's earlier discussion of policies and regulations found in Chapter III.

A. National Institute of Standards and Technology (NIST)
   1. Areas of Responsibility
      - Develop standards (i.e., DES, POSIX, Network Security)
      - Provide guidance and training
      - Operate within internal agreement with NSA on policy development
      - Assist agencies to achieve C2 by 1992

   2. Impact on Federal Computer Security Market
      - Develops additional requirements
      - Centers more attention on standards than security
      - Increases awareness/compliance
      - Promotes implementation of off-the-shelf technology

B. National Security Agency (NSA)
   1. Areas of Responsibility
      - Define security protocols
      - Monitor product evaluation/certification process
      - Concentrate efforts in DoD and classified areas
      - Assist with technical problems and security issues related to national security

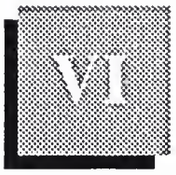
2. Impact on Federal Computer Security Market
   - Need to simplify product evaluation process
   - Develops additional access control requirements
   - Need to improve coordination efforts with industry and NIST
   - Increases agency use of security products

C. General Services Administration (GSA)
   1. Areas of Responsibility
      - Evaluate A, B, C security categories to promote more effective use of hardware and software
      - Establish procurement regulations
      - Assist with establishing federal security policies
      - Mandate security planning for agency DPAs (Delegations of Procurement Authority)

   2. Impact on Federal Computer Security Market
      - Influences size of procurements
      - Compounds problem of MLS/Interoperability
      - Need stricter enforcement of standards
      - Minimal impact on security
      - Increases agency use of security products

Industry respondents viewed the activities and assistance provided by each of these agencies as mostly beneficial. However, they expressed some frustration as a result of conflicts in attempting to comply with a variety of standards and requirements developed by the policy-formulating agencies studied. The comments received by the vendors are similar to those of the agency respondents summarized in Exhibit IV-22. Both groups of respondents view NSA as taking the leading role in product evaluation and GSA as having the least impact overall.

In the future, new legislation will likely clarify the roles of the various oversight agencies. There are currently too many ambiguities in responsibilities, leaving both agencies and vendors somewhat bewildered about who is really in charge.



Key Opportunities

This section describes specific opportunities in the federal information technology market.

Although this opportunity list is not all-inclusive, it includes major programs typical of the federal market.

This list of opportunities becomes smaller after FY 1990 because new programs have not yet been identified or initially approved by the responsible agency. Subsequent issues of this report and the INPUT Procurement Analysis Reports will include additional programs and detailed program information for FY 1990 - FY 1995.

A

Present and Future Programs

New information technology programs larger than $1-2 million are listed in at least one of the following federal government documents:

OMB/GSA Five-Year Plan, which is developed from agency budget requests submitted in compliance with OMB Circular A-ll.

Agency long-range information resource plans developed to meet the reporting requirements of the Paperwork Reduction Reauthorization Act of 1986.

Agency annual operating budget requests submitted to congressional oversight and appropriations committees based on the OMB A-ll information.

Commerce Business Daily for specific opportunities for qualifications as a bidder, and invitations to submit a bid in response to an RFP or RFQ.

Five-Year Defense Plan, which is not publicly available, and the supporting documentation of the separate military departments and agencies.

Classified program documentation available only to qualified DoD contractors.

Opportunities related to computer security may not be specifically identified as such in these documents. Information technology planning documents usually identify mission requirements to be met by specific programs, rather than methods for meeting those requirements. An agency decision to use a computer security contractor may not be made until a program is well under way and an acquisition plan has been formulated. Over the last several years, however, agencies have shown an increasing tendency to use systems engineering and integration contractors for larger, more complex systems.

All funding proposals are based on cost data of the year submitted, with inflation factors dictated by the Administration as part of its fiscal policy, and are subject to revision, reduction, or spread to future years in response to congressional direction. Some additional reductions will be likely in FY 1991 and beyond, due to the tightening of the Department of Defense budget.

B

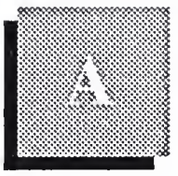
Computer Security Opportunities by Agency

Agency/Program	PAR Reference	RFP Schedule	FY1990- FY1995 Funding (Est. $ Millions)
Air Force			
AF WWMCCS ADP Modernization (AFWAM)	V-1-27	UNK	164
Survivable Base Recovery After Attack (BRAAT) Communications System (SBCS)	V-1-120	11/90	UNK
Tactical Air Force Workstations—AFCAC 308	V-1-134	FY91/92	UNK
Continuous Engineering and Technical Services	V-1-134	FY91/92	163

Agency/Program	PAR Reference	RFP Schedule	FY1990- FY1995 Funding (Est. $ Millions)
Army			
Army WWMCCS Information System (AWIS)	V-2-8	4Q/FY90	UNK
Army Tactical Command and Control System (ATCCS)	V-2-38	7/90	UNK
Command Hardware/Software II (CHS-II)	V-2-51	7/91	2,000
Navy			
Navy WWMCCS ADP Modernization (Navy WAM)	V-3-83	UNK	13
Remote Information Exchange Terminal (RIXT) System	V-3-93	5/90	200
PMTC Support Services	V-3-108	4Q/FY90	50
Marines			
Marine Air Ground Task Force (MAGTF) Automated Services Center (MASC)	V-3A-4	FY92	UNK
Defense Communications Agency			
Joint Operations Planning and Execution System (JOPES)	V-4G-5	4Q/FY90	250
Integrated Defense Communications System—Western Hemisphere (IDCS-WH)	V-4G-6	FY91	10,000

Agency/Program	PAR Reference	RFP Schedule	FY1990- FY1995 Funding (Est. $ Millions)
Defense Intelligence Agency (DIA)			
Compartmented Mode Workstation	V-4H-1	UNK	UNK
Commerce			
Upgrade/Enhance Gateway Computer Systems	VI-6-30	6/90	6
Energy			
National Waste Information Network	VI-7-85	FY91	UNK
ADP Support Services	VI-7-93	FY92	15
Labor			
BLS Contract for Host Computer Services	VII-9A-10	FY93	33
Justice			
FBI Field Office Information Management System	VII-10-2	UNK	530
Computer Applications Communications Network	VII-10-9	UNK	157
National Crime Information Center (NCIC) Upgrade	VII-10-24	UNK	143
Computer Assisted Dispatch and Reporting Enhancement II (CADRE II)	VII-10-27	UNK	25

Agency/Program	PAR Reference	RFP Schedule	FY1990- FY1995 Funding (Est. $ Millions)
Treasury			
Tax Modernization Effort	VII-12-6	UNK	297
Treasury Enforcement Communications System (TECS II)	VII-12-56	4Q/FY90	153
Corporate Files On-Line (CFOL) and Corporate Systems/Mirror Imaging Acquisition (CS/MIA)	VII-12-66	1/91	727
NASA			
Kennedy Switched Data Network	VIII-15-72	UNK	UNK
Program Support Communications Network	VIII-15-73	FY94	UNK
NASCOM Augmentation	VIII-15-89	1/91	UNK



Appendix: Federal Computer Security Market Interview Profiles

A

Federal Agency Respondent Profile

Contacts with agencies were made both by mail and telephone. The following agencies were interviewed:

Department of Air Force
Department of Army
Department of Commerce
Defense Technical Information Center
Department of Energy
General Accounting Office
Department of Health and Human Services
- Food and Drug Administration
- Public Health Service

Department of Housing and Urban Development
Department of Interior
Department of Justice
- U.S. Marshal Service

NASA
Department of the Navy
- Naval Supply Systems Command
- Naval Weapons Center

Office of Secretary of Defense
Smithsonian Institute
Supreme Court of the United States
Department of Treasury
- Internal Revenue Service

Interviews included program managers and agency policy officials.

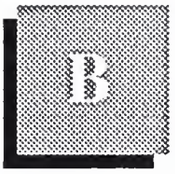
B

Vendor Respondent Profile

INPUT contacted a representative sample of contractors that currently provide or plan to provide computer security products and services to the federal government.

Job classifications among individual vendor respondents included marketing, program managers, and administrative executives.

Interviews with vendor personnel were conducted by telephone and by mail.



Definitions

The definitions in this appendix include hardware, software, services, and telecommunications categories to accommodate the range of information systems and services programs described in this report.

Alternate service mode terminology employed by the federal government in its procurement process is defined along with INPUT's regular terms of reference, as shown in Exhibit B-1.

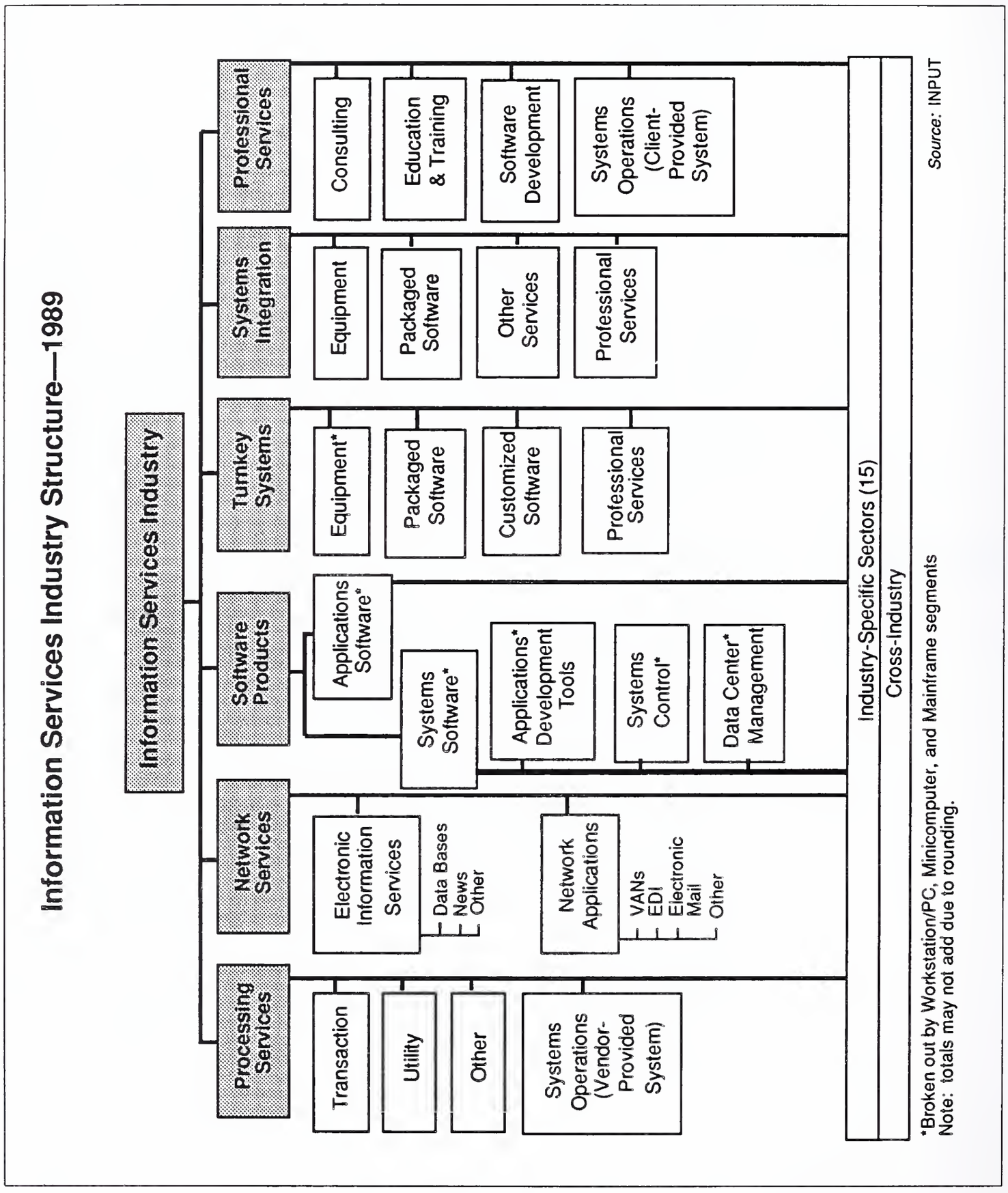
A
Delivery Modes

1. Processing Services

This category includes transaction processing, utility processing, other processing services, and processing facilities management.

- *Transaction Processing Services* - Updates client-owned data files by entry of specific business activity, such as sales order, inventory receipt, cash disbursement, etc. Transactions may be entered in one of three modes.
  - *Interactive* - Characterized by the interaction of the user with the system, primarily for problem-solving timesharing, but also for data entry and transaction processing; the user is on-line to the program files. Computer response is usually measured in seconds or fractions of a second.
  - *Remote Batch* - Where the user hands over control of a job to the vendor's computer, which schedules job execution according to priorities and resource requirements. Computer response is measured in minutes or hours.

EXHIBIT B-1



"Other" Processing Services include:

- *Batch Services* - These include data processing at vendors' sites for user programs and/or data that are physically transported (as opposed to transported electronically by telecommunications media) to and/or from those sites. Data entry and data output services, such as keypunching and computer output microfilm processing, are also included. Batch services include expenditures by users who take their data to a vendor site that has a terminal connected to a remote computer for the actual processing. Other services also includes disaster recovery and backup services.

- *Systems Operations (Processing)* - Also referred to as "Resource Management," Facilities Management or "COCO" (contractor-owned, contractor-operated). Systems control is the management of all or part of a user's data processing functions under a long-term contract of not less than one year. This would include remote computing and batch services. To qualify, the contractor must directly plan, control, operate, and own the facility provided to the user–either on-site, through communications lines, or in a mixed mode.

2. Network Services

Include a wide variety of network-based functions and operations. The common thread is that none of these functions could be performed without network involvement. Network services is divided into two segments: value-added networks (enhanced services), and network applications (electronic information systems).

- *Value-Added Networks (VANs)* - VANs typically involve common carrier network transmission facilities that are augmented with computerized switches. These networks have become associated with packet-switching technology because the public VANs that have received the most attention (e.g., Telenet and TYMNET) employ packet-switching techniques. However, other added data service features such as store-and-forward message switching, terminal interfacing, error detection and correction, and host computer interfacing are of equal importance.

- *Network applications* include electronic data interchange (EDI), the application-to-application electronic communications between organizations, based on established business document standards and electronic mail.

3. Software Products

This category includes user purchases of applications and systems software packages for in-house computer systems. Included are lease and purchase expenditures, as well as expenditures for work performed by the

vendor to implement or maintain the package at the user's sites. Expenditures for work performed by organizations other than the package vendor are counted in the category of professional services. Fees for work related to education, consulting, and/or custom modification of software products are counted as professional services, provided such fees are charged separately from the price of the software product itself. There are several subcategories of software products, as indicated below and shown in detail in Exhibit B-2.

- *Applications Products* - Software that performs functions directly related to solving user's business or organizational need. The products can be:
  - *Cross-Industry Products* - Used in multiple-industry applications as well as the federal government sector. Examples are payroll, inventory control, and financial planning.
  - *Industry-Specific Products* - Used in a specific industry sector, such as banking and finance, transportation, or discrete manufacturing. Examples are demand deposit accounting, airline scheduling, and material resource planning.
- *Systems Software Products* - Software that enables the computer/communications system to perform basic functions. These products include:
  - *System Control Products* - Function during applications program execution to manage the computer system resources. Examples include operating systems, communication monitors, emulators, spoolers, network control, library control, windowing, access control.
  - *Data Center Management Products* - Used by operations personnel to manage computer systems resources and personnel more effectively. Examples include performance measurement, job accounting, computer operations scheduling, utilities, capacity management.
  - *Applications Development Products* - Used to prepare applications for execution by assisting in designing, programming, testing, and related functions. Examples include traditional programming languages, 4GLs, sorts, productivity aids, assemblers, compilers, data dictionaries, data base management systems, report writers, project control, and CASE systems.

4. Professional Services

This category includes consulting, education and training, software development, and systems operations as defined below.

- *Software Development* - Develops a software system on a custom basis. It includes one or more of the following: user requirements definition, system design, contract programming, documentation, and software maintenance.

- *Education and Training* - Products and/or services related to information systems and services for the user, including computer-aided instruction (CAI), computer-based education (CBE), and vendor instruction of user personnel in operations, programming, and maintenance.

- *Consulting Services* - Information systems and/or services management consulting, project assistance (technical and/or management), feasibility analyses, and cost-effectiveness trade-off studies.

- *Systems Operations (Professional Services)* - This is a counterpart to systems operations (processing services) except the computing equipment is owned or leased by the client, not by the vendor. The vendor provides the staff to operate, maintain, and manage the client's facility.

5. Turnkey Systems

A turnkey system is an integration of systems and applications software with CPU hardware and peripherals, packaged as a single application (or set of applications) solution. The value added by the vendor is primarily in the software and support. Most CAD/CAM systems and many small-business systems are turnkey systems. This does not include specialized hardware systems such as word processors, cash registers, or process control systems, nor does it include Embedded Computer Resources for military applications. Turnkey systems may be either custom or packaged systems.

- Hardware vendors that combine software with their own general-purpose hardware are not classified by INPUT as turnkey vendors. Their software revenues are included in the appropriate software category.

- Turnkey systems revenue is divided into two categories:

  - *Industry-specific systems* - that is, systems that serve a specific function for a given industry sector such as automobile dealer parts inventory, CAD/CAM systems, or discrete manufacturing control systems.

EXHIBIT B-2

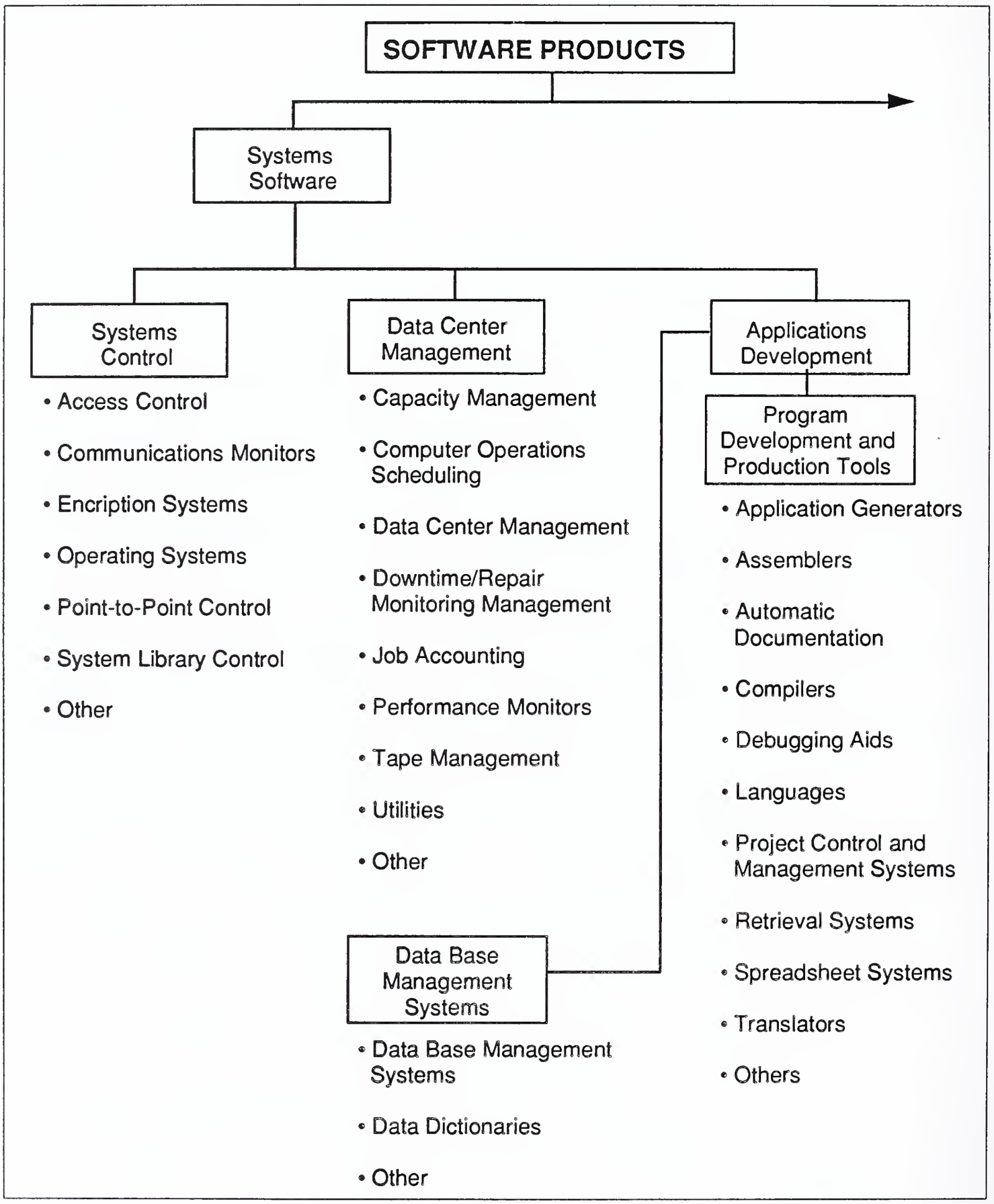
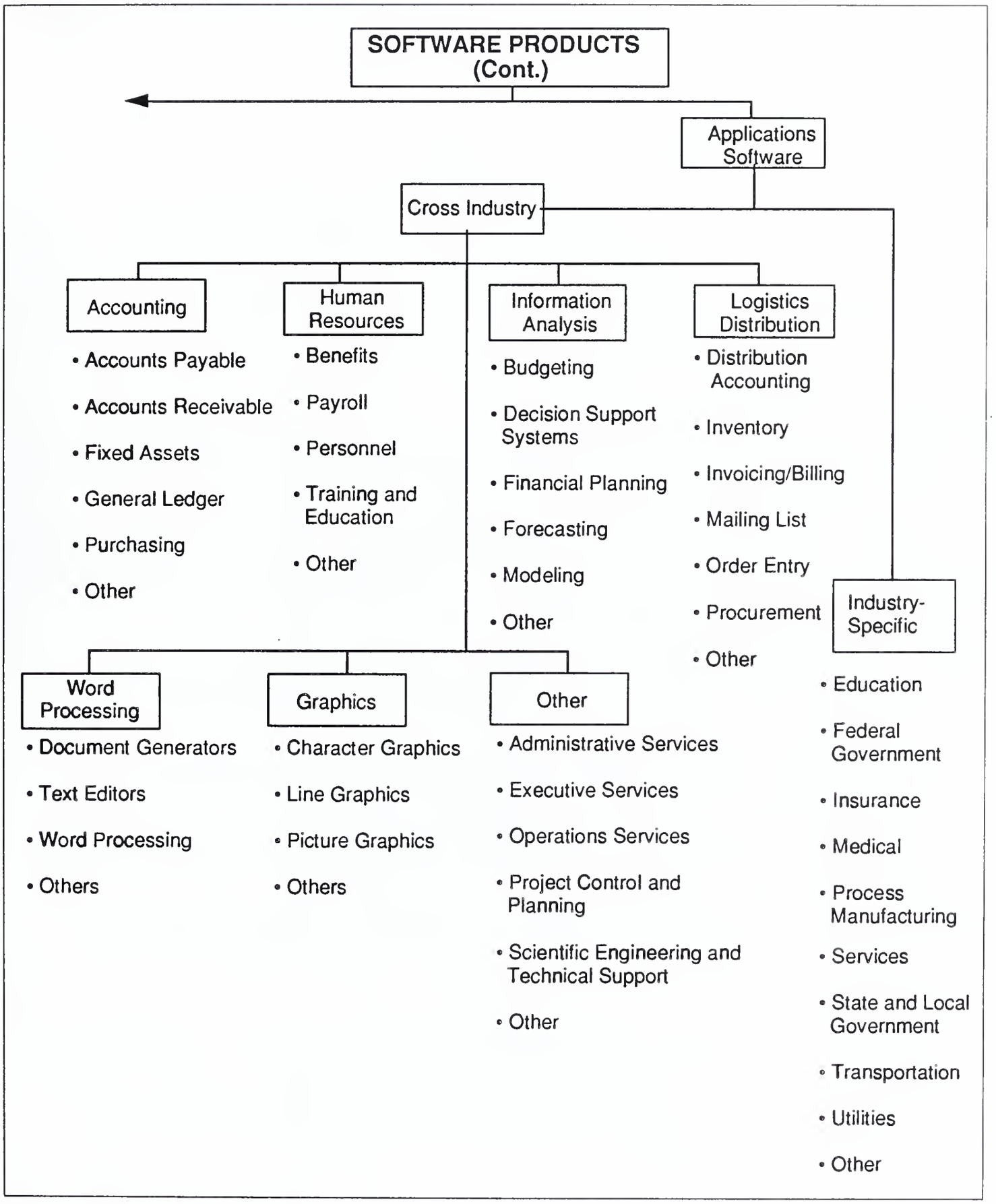


EXHIBIT B-2 (Cont.)



- *Cross-industry systems* - that is, systems that provide a specific function that is applicable to a wide range of industry sectors such as financial planning systems, payroll systems, or personnel management systems.

• Revenue includes hardware, software, and support functions.

6. Systems Integration (SI)

Delivery of large, complex multidisciplinary, multivendor systems, incorporating some or all of these categories: systems design, programming, integration, equipment, packaged software, communication networks, installation education and training, and SI-related professional services and acceptance. Systems integration contracts typically take more than a year to complete and involve a prime contractor assuming risk and accepting full responsibility.

B

Hardware/Hardware Systems

Hardware - Includes all computer and telecommunications equipment that can be separately acquired with or without installation by the vendor and not acquired as part of an integrated system.

• *Peripherals* - Includes all input, output, communications, and storage devices (other than main memory) that can be connected locally to the main processor, and generally cannot be included in other categories such as terminals.

• *Input Devices* - Includes keyboards, numeric pads, card readers, light pens and track balls, tape readers, position and motion sensors, and analog-to-digital converters.

• *Output Devices* - Includes printers, CRTs, projection television screens, micrographics processors, digital graphics, and plotters.

• *Communication Devices* - Includes modems, encryption equipment, special interfaces, and error control.

• *Storage Devices* - Includes magnetic tape (reel, cartridge, and cassette), floppy and hard disks, solid state (integrated circuits), and bubble and optical memories.

Hardware Systems - Includes all processors from microcomputers to supercomputers. Hardware systems may require type- or model-unique operating software to be functional, but this category excludes applications software and peripheral devices, other than main memory and processors or CPUs not provided as part of an integrated (turnkey) system.

- *Microcomputer* - Combines all of the CPU, memory, and peripheral functions of an 8-, 16-, or 32-bit computer on a chip in the form of:

  - Integrated circuit package
  - Plug-in boards with more memory and peripheral circuits
  - Console including keyboard and interfacing connectors
  - Personal computer with at least one external storage device directly addressable by the CPU
  - An embedded computer which may take a number of shapes or configurations

  Microcomputers are primarily single-user computers that cost under $15,000.

- *Midsize Computer* - Typically a 32- or 64-bit computer with extensive applications software and a number of peripherals in standalone or multiple-CPU configurations for business (administrative, personnel, and logistics) applications; also called a general-purpose computer. Specific systems in this category are: IBM 93XX systems, all Digital VAX series systems, and such common UNIX-based systems as from Apollo and Sun) are also included. Most large shared-logic, integrated office systems-such as those from Wang, Hewlett-Packard, and Groupe Bull would also be considered midsize systems. Does not include microcomputers (standalone, or shared), embedded systems, and CAD/CAM systems.

- *Large Computer* - Presently centered around storage controllers but likely to become bus-oriented and to consist of multiple processors or parallel processors. Intended for structured mathematical and signal processing and typically used with general-purpose, VonNeumann-type processors for system control. Usually refers to traditional mainframes (such as IBM 30XX, Unisys (Sperry) 1100/XX, Honeywell DDPS88, Unisys (Burroughs) A15, or CDC Cyber series) and supercomputers (such as products from Cray, ETA, Fujitsu, and the new IBM development effort).

- *Supercomputer* - High-powered processors with numerical processing throughput that is significantly greater than the fastest general-purpose computers, with capacities in the 100-500 million floating point operations per second (MFLOPS) range. Newer supercomputers, with burst modes over 500 MFLOPS, main storage size up to 10 million words, and on-line storage in the one-to-three gigabyte class, are labeled Class IV to Class VII in agency long-range plans.

C

Telecommunications

Networks - Electronic interconnection between sites or locations that may incorporate links between central computer sites and remote locations and switching and/or regional data processing nodes. Network services typically are provided on a leased basis by a vendor to move data, voice, video, or textual information between locations. Networks can be categorized in several different ways.

- *Common Carrier Network* - A public access network, such as provided by AT&T, consisting of conventional voice-grade circuits and regular switching facilities accessed through dial-up calling with leased or user-owned modems for transfer rates between 150 and 1200 baud.

- *Value-Added Network (VAN)* - (See listing under Section 2, Network Services.)

- *Local-Area Network (LAN)* - Limited-access network between computing resources in a relatively small (but not necessarily contiguous) area, such as a building, complex of buildings, or buildings distributed within a metropolitan area. Uses one of two signaling methods:

- *Wide-Area Network (WAN)* - Limited access network between computing resources in buildings, complexes of buildings, or buildings within a large metropolitan or wide geographical area. Uses baseband or broadband signaling methods.

D

General Definitions

ASCII - American National Standards Code for Information Interchange-eight-bit code with seven data bits and one parity bit.

Asynchronous - Communications operation (such as transmission) without continuous timing signals. Synchronization is accomplished by appending signal elements to the data.

Benchmark - Method of testing proposed ADP system solutions for a specified set of functions (applications) employing simulated or real data inputs under simulated operating conditions.

CBX - Computerized Branch Exchange - a PABX based on a computer system, implying programmability and usually voice and data capabilities.

Central Processing Unit (CPU) - The arithmetic and control portion of a computer; i.e., the circuits controlling the interpretation and execution of computer instructions.

Computer System - The combination of computing resources required to perform the designed functions and which may include one or more CPUs, machine room peripherals, storage systems, and/or applications software.

Data Encryption Standard (DES) - 56-bit key, one-way encryption algorithm adopted by NBS in 1977, implemented through hardware ("S-boxes") or software. Designed by IBM with NSA guidance.

Distributed Data Processing - The development of programmable intelligence in order to perform a data processing function where it can be accomplished most effectively through computers and terminals arranged in a telecommunications network adapted to the user's characteristics.

Encryption - Electrical, code-based conversion of transmitted data to provide security and/or privacy of data between authorized access points.

End User - One who is using a product or service to accomplish his or her own functions. The end user may buy a system from the hardware supplier(s) and do his or her own programming, interfacing, and installation. Alternately, the end user may buy a turnkey system from a systems house or hardware integrator, or may buy a service from an in-house department or external vendor.

Facsimile - Transmission and reception of data in graphic form, usually fixed images of documents, through scanning and conversion of a picture signal.

Information Processing - Data processing as a whole, including use of business and scientific computers.

Installed Base - Cumulative number or value (cost when new) of computers in use.

Interconnection - Physical linkage between devices on a network.

Interoperability - The capability to operate with other devices on a network. To be contrasted with interconnection, which merely guarantees a physical network interface.

ISDN - Integrated Services Digital Network - integrated voice and non-voice public network service which is completely digital. Not clearly defined through any existing standards although FCC and other federal agencies are participating in the development of CCITT recommendations.

Mainframe - The central processing unit (CPU or units in a parallel processor) of a computer that interprets and executes computer (software) instructions of 32 bits or more. Usually refers to traditional mainframes (such as IBM 30XX, Unisys (Sperry) 1100/XX, Honeywell DDPS88, Unisys (Burroughs) A15, or CDC (Cyber series).

Modem - A device that encodes information into electronically transmittable form (MOdulator) and restores it to original analog form (DEModulator).

OSI - ISO reference model for Open Systems Interconnection - seven-layer architecture for application, presentation, session, transport, network, data link, and physical services and equipment.

OSI Application Layer - Layer 7, providing end-user applications services for data processing.

OSI Data Link Layer - Layer 2, providing transmission protocols, including frame management, link flow control, and link initiation/release.

OSI Network Layer - Layer 3, providing call establishment and clearing control through the network nodes.

OSI Physical Layer - Layer 1, providing the mechanical, electrical, functional, and procedural characteristics to establish, maintain, and release physical connections to the network.

OSI Presentation Layer - Layer 6, providing data formats and information such as data translation, data encoding/decoding, and command translation.

OSI Session Layer - Layer 5, establishes, maintains, and terminates logical connections for the transfer of data between processes.

OSI Transport Layer - Layer 4, providing end-to-end terminal control signals such as acknowledgements.

PDN - Public Data Network - a network established and operated by a recognized private operating agency, a telecommunications administration, or other agency for the specific purpose of providing data transmission services to the public.

Program Network - A network established and operated for one user or user organization.

Programmers - Persons mainly involved in designing, writing, and testing of computer software programs.

Protocols - The rules for communication system operation that must be followed if communication is to be effected. Protocols may govern portions of a network or service. In digital networks, protocols are digitally encoded as instructions to computerized equipment.

Public Network - A network established and operated for more than one user with shared access, usually available on a subscription basis. See related international definition of PDN.

Security - Physical, electrical, and computer (digital) coding procedures to protect the contents of computer files and data transmission from inadvertent or unauthorized disclosure to meet the requirements of the Privacy Act and national classified information regulations.

Software - Computer programs.

Systems House - Vendor that acquires, assembles, and integrates hardware and software into a total system to satisfy the data processing requirements of an end user. The vendor also may develop systems software products for license to end users. The systems house vendor does not manufacture mainframes.

Systems Integrator - Systems house vendor that develops systems interface electronics, applications software, and controllers for the CPU, peripherals, and ancillary subsystems that may have been provided by a contractor or the government (GFE). This vendor may either supervise or perform the installation and testing of the completed system.

Verification and Validation - Process for examining and testing applications and special systems software to verify that it operates on the target CPU and performs all of the functions specified by the user.

E

Other Considerations

When questions arise as to the proper place to count certain user expenditures, INPUT addresses the questions from the user viewpoint. Expenditures then are categorized according to what the users perceive they are buying.

F

Computer Security Terms

The following glossary of computer security terms is taken from *Department of Defense Trusted Computer System Evaluation Criteria,* dated 15 August, 1983. This publication is popularly referred to as "The Orange Book".

GLOSSARY

Access - A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

Approval/Accreditation - The official authorization that is granted to an ADP system to process sensitive information in its operational environment, based upon comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration, and

implementation, and of the other system procedural, administrative, physical, Tempest, personnel, and communications security controls.

Audit Trail - A set of records that collectively provide documentary evidence of processing, used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions.

Authenticate - To establish the validity of a claimed identity.

Automatic Data Processing (ADP) System - An assembly of computer hardware, firmware, and software configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.

Bandwidth - A characteristic of a communication channel that is the amount of information that can be passed through it in a given amount of time, usually expressed in bits per second.

Bell-LaPadula Model - A formal state transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of a secure state is defined and it is proven that each state transition preserves security by moving from secure state to secure state; thus, inductively proving that the system is secure. A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object and a determination is made as to whether the subject is authorized for the specific access mode. The clearance/classification scheme is expressed in terms of a lattice. See also: Lattice, Simple Security Property, *Property.

Certification - The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular computer system's design and implementation meet a set of specific security requirements.

Channel - An information transfer path within a system. May also refer to the mechanism by which the path is effected.

Covert Channel - A communication channel that allows a process to transfer information in a manner that violates the system's security policy. See also: Covert Storage Channel, Covert Timing Channel.

Covert Storage Channel - A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Covert Timing Channel - A covert channel in which one process signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process.

Data - Information with a specific physical representation.

Data Integrity - The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

Descriptive Top-Level Specification (DTLS) - A top-level specification that is written in a natural language (e.g., English), an informal program design notation, or a combination of the two.

Discretionary Access Control - A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Domain - The set of objects that a subject has the ability to access.

Dominate - Security level S1 is said to dominate security level S2 if the hierarchical classification of S1 is greater than or equal to that of S2 and the non-hierarchical categories of S1 include all those of S2 as a subset.

Exploitable Channel - Any channel that is useable or detectable by subjects external to the Trusted Computing Base.

Flaw Hypothesis Methodology - A system analysis and penetration technique where specifications and documentation for the system are analyzed and then flaws in the system are hypothesized. The list of hypothesized flaws is then prioritized on the basis of the estimated probability that a flaw actually exists and, assuming a flaw does exist, on the ease of exploiting it and on the extent of control or compromise it would provide. The prioritized list is used to direct the actual testing of the system.

Flaw - An error of commission, omission, or oversight in a system that allows protection mechanisms to be bypassed.

Formal Proof - A complete and convincing mathematical argument, presenting the full logical justification for each proof step, for the truth of a theorem or set of theorems. The formal verification process uses formal proofs to show the truth of certain properties of formal specification and for showing that computer programs satisfy their specifications.

Formal Security Policy Model - A mathematically precise statement of a security policy. To be adequately precise, such a model must represent the initial state of a system, the way in which the system progresses from one state to another, and a definition of a "secure" state of the system. To be acceptable as a basis for a TCB, the model must be supported by a formal proof that if the initial state of the system satisfies the definition of a "secure" state and if all assumptions required by the model hold, then all future states of the system will be secure. Some formal modeling techniques include: state transition models, temporal logic models, denotational semantics models, algebraic specification models. An example is the model described by Bell and LaPadula in reference [2]. See also: Bell-LaPadula Model, Security Policy Model.

Formal Top-Level Specification (FTLS) - A Top-Level Specification that is written in a formal mathematical language to allow theorems showing the correspondence of the system specification to its formal requirements to be hypothesized and formally proven.

Formal Verification - The process of using formal proofs to demonstrate the consistency (design verification) between a formal specification of a system and a formal security policy model or (implementation verification) between the formal specification and its program implementation.

Functional Testing - The portion of security testing in which the advertised features of a system are tested for correct operation.

General-Purpose System - A computer system that is designed to aid in solving a wide variety of problems.

Lattice - A partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound.

Least Privilege - This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Mandatory Access Control - A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity.

Multilevel Device - A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, sensitivity labels are normally stored on the same physical medium and in the same form (i.e., machine-readable or human-readable) as the data being processed.

Multilevel Secure - A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization.

Object - A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc.

Object Reuse - The reassignment to some subject of a medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. To be securely reassigned, such media must contain no residual data from the previously contained object(s).

Output - Information that has been exported by a TCB.

Password - A private character string that is used to authenticate an identity.

Penetration Testing - The portion of security testing in which the penetrators attempt to circumvent the security features of a system. The penetrators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The penetrators work under no constraints other than those that would be applied to ordinary users.

Process - A program in execution. It is completely characterized by a single current execution point (represented by the machine state) and address space.

Protection-Critical Portions of the TCB - Those portions of the TCB whose normal function is to deal with the control of access between subjects and objects.

Protection Philosophy - An informal description of the overall design of a system that delineates each of the protection mechanisms employed. A combination (appropriate to the evaluation class) of formal and informal techniques is used to show that the mechanisms are adequate to enforce the security policy.

Read - A fundamental operation that results only in the flow of information from an object to a subject.

Read Access - Permission to read information.

Reference Monitor Concept - An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

Resource - Anything used or consumed while performing a function. These categories of resources are: time, information, objects (information containers), or processors (the ability to use information). Specific examples are: CPU time; terminal connect time; amount of directly-addressable memory; disk space; number of I/O requests per minute, etc.

Security Kernel - The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

Security Level - The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.

Security Policy - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Policy Model - An informal presentation of a formal security policy model.

Security Testing - A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification. See also: Functional Testing, Penetration Testing, Verification.

Sensitive Information - Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.

Sensitivity Label - A piece of information that represents the security level of an object and that describes the sensitivity (e.g., classification) of the data in the object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions.

Simple Security Property - A Bell-LaPadula security model rule allowing a subject read access to an object only if the security level of the subject dominates the security level of the object.

Single-Level Device - A device that is used to process data of a single security level at any one time. Since the device need not be trusted to separate data of different security levels, sensitivity labels do not have to be stored with the data being processed.

**Property (Star Property)* - A Bell-LaPadula security model rule allowing a subject write access to an object only if the security level of the subject is dominated by the security level of the object. Also known as the Confinement Property.

Storage Object - An object that supports both read and write accesses.

Subject - An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair.

Subject Security Level - A subject's security level is equal to the security level of the objects to which it has both read and write access. A subject's security level must always be dominated by the clearance of the user the subject is associated with.

Tempest - The study and control of spurious electronic signals emitted from ADP equipment.

Top-Level Specification (TLS) - A non-procedural description of system behavior at the most abstract level. Typically a functional specification that omits all implementation details.

Trap Door - A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner (e.g., special "random" key sequence at a terminal).

Trojan Horse - A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. For example, making a "blind copy" of a sensitive file for the creator of the Trojan Horse.

Trusted Computer System - A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

Trusted Computing Base (TCB) - The totality of protection mechanisms within a computer system—including hardware, firmware, and software—the combination of which is responsible for enforcing a security policy. It creates a basic protection environment and provides additional user services required for a trusted computer system. The ability of a

trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel or parameters (e.g., a user's clearance) related to the security policy.

Trusted Path - A mechanism by which a person at a terminal can communicate directly with the Trusted Computing Base. This mechanism can only be activated by the person or the Trusted Computing Base and cannot be imitated by untrusted software.

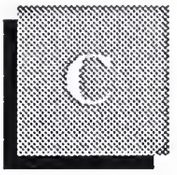
Trusted Software - The software portion of a Trusted Computing Base.

User - Any person who interacts directly with a computer system.

Verification - The process of comparing two levels of system specification for proper correspondence (e.g., security policy model with top-level specification, TLS with source code, or source code with object code). This process may or may not be automated.

Write - A fundamental operation that results only in the flow of information from a subject to an object.

Write Access - Permission to write an object.



Appendix: Glossary of Acronyms

The federal government's procurement language uses a combination of acronyms, phrases, and words that is complicated by different agency definitions and interpretations. The government also uses terms of accounting, business, economics, engineering, and law with new applications and technology.

Acronyms and contract terms that INPUT encountered most often in program documentation and interviews for this report are included here, but this glossary should not be considered all-inclusive. Federal procurement regulations (DAR, FPR, FAR, FIRMR, FPMR) and contract terms listed in RFIs, RFPs, and RFQs provide applicable terms and definitions.

Federal agency acronyms have been included to the extent they are employed in this report or applicable to the federal computer security market.

A

Federal Acronyms

ADL	Authorized Data List.
ADS	Automatic Digital Switches (DCS).
AFCEA	Armed Forces Communications Electronics Association.
AIS	Automated Information System.
AMPE	Automated Message Processing Equipment.
AMPS	Automated Message Processing System.
Appropriation	Congressionally approved funding for authorized programs and activities of the Executive Branch.
APR	Agency Procurement Request.
ARPANET	DARPA network of scientific computers.
Authorization	In the legislative process programs, staffing, and other routine activities must be approved by Oversight Committees before the Appropriations Committee will approve the money from the budget.

BCA	Board of Contract Appeals.
Benchmark	Method of evaluating ability of a candidate computer system to meet user requirements.
Bid Protest	Objection (in writing, before or after contract award) to some aspect of a solicitation by a valid bidder.
BML	Bidders Mailing List - qualified vendor information filed annually with federal agencies to automatically receive RFPs and RFQs in areas of claimed competence.
BOA	Basic Ordering Agreement.
B&P	Bid and Proposal - vendor activities in response to government solicitation/specific overhead allowance.
BPA	Blanked Purchase Agreement.
Budget	Federal Budget, proposed by the President and subject to Congressional review.
C2	Command and Control.
C3	Command, Control, and Communications.
C4	Command, Control, Communications, and Computers.
C3I	Command, Control, Communications, and Intelligence.
CALS	Computer-Aided Automated Logistic System.
CBD	Commerce Business Daily - U.S. Department of Commerce publication listing government contract opportunities and awards.
CBO	Congressional Budget Office.
CCEP	Commercial Comsec Endorsement Program.
CCDR	Contractor Cost Data Reporting.
CFR	Code of Federal Regulations.
CICA	Competition in Contracting Act.
DAR	Defense Acquisition Regulations.
DARPA	Defense Advanced Research Projects Agency.
DAS	Data Acquisition System.
DBHS	Data Base Handling System.
DCA	Defense Communications Agency.
DCAA	Defense Contract Audit Agency.
DCAS	Defense Contract Administration Services.
DDL	Digital Data Link - A segment of a communications network used for data transmission in digital form.
DDN	Defense Data Network.
DIA	Defense Intelligence Agency.
DIF	Document Interchange Format, Navy-sponsored word processing standard.

DHHS	Department of Health and Human Services.
DIDS	Defense Integrated Data Systems.
DLA	Defense Logistics Agency.
DMA	Defense Mapping Agency.
DNA	Defense Nuclear Agency.
DO	Delivery Order.
DOA	Department of Agriculture (also USDA).
DOC	Department of Commerce.
DOE	Department of Energy.
DOI	Department of Interior.
DOJ	Department of Justice.
DOS	Department of State.
DOT	Department of Transportation.
DPA	Delegation of Procurement Authority (granted by GSA under FPRs).
ED	Department of Education.
EEO	Equal Employment Opportunity.
8(a) Set-Aside	Agency awards direct to Small Business Administration for direct placement with a socially/economically disadvantaged company.
EO	Executive Order - Order issued by the President.
EOQ	Economic Ordering Quantity.
EUC	End User Computing, especially in DoD.
FAR	Federal Acquisition Regulations.
FCC	Federal Communications Commission.
FCDC	Federal Contract Data Center.
FCRC	Federal Contract Research Center.
FDPC	Federal Data Processing Center.
FEDSIM	Federal (Computer) Simulation Center (GSA).
FEMA	Federal Emergency Management Agency.
FIPS	NBS Federal Information Processing Standard.
FIPS PUBS	FIPS Publications.
FIRMR	Federal Information Resource Management Regulations.
FOIA	Freedom of Information Act.
FPMR	Federal Property Management Regulations.
FPR	Federal Procurement Regulations.
FSC	Federal Supply Classification.
FSTS	Federal Secure Telecommunications System.
FT Fund	A revolving fund, designated as the Federal Telecommunications Fund, used by GSA to pay for GSA-provided common-user services, specifically including the current FTS and proposed FTS 2000 services.

FTSP	Federal Telecommunications Standards Program administered by NCS; Standards are published by GSA.
FTS	Federal Telecommunications System.
FTS 2000	Replacement for the Federal Telecommunications System.
FY	Fiscal Year.
FYDP	Five-Year Defense Plan.
GAO	General Accounting Office.
GFY	Government Fiscal Year (October to September).
GOCO	Government-Owned, Contractor-Operated.
GOGO	Government-Owned, Government-Operated.
GOSIP	Government Open Systems Interconnection Profile.
GPO	Government Printing Office.
GRH	Gramm-Rudman-Hollings Act (1985), also called Gramm-Rudman Deficit Control.
GSA	General Services Administration.
GSBCA	General Services Administration Board of Contract Appeals.
HCFA	Health Care Financing Administration.
HHS	(Department of) Health and Human Services.
HSDP	High-Speed Data Processors.
HUD	(Department of) Housing and Urban Development.
ICAM	Integrated Computer-Aided Manufacturing.
ICE	Independent Cost Estimate.
ICST	Institute for Computer Sciences and Technology, National Institute of Standards and Technology, Department of Commerce.
IDN	Integrated Data Network.
IFB	Invitation For Bids.
IPS	Integrated Procurement System.
IQ	Indefinite Quantity Contract.
IRM	Information Resources Management.
IXS	Information Exchange System.
JSIPS	Joint Systems Integration Planning Staff.
JSOR	Joint Service Operational Requirement.
JUMPS	Joint Uniform Military Pay System.
LC	Letter Contract.
LCC	Life Cycle Costing.
LCMP	Life Cycle Management Procedures (DD7920.1).
LCMS	Life Cycle Management System.
LRPE	Long-Range Procurement Estimate.
LRIRP	Long-Range Information Resource Plan.

MAISRC	Major Automated Information Systems Review Council (DoD).
MANTECH	MANufacturing TECHnology.
MAPS	Multiple Address Processing System.
MAP/TOP	Manufacturing Automation Protocol/Technical and Office Protocol.
MENS	Mission Element Need Statement or Mission Essential Need Statement (See DD-5000.1 Major Systems Acquisition).
MILSCAP	Military Standard Contract Administration Procedures.
MIL SPEC	Military Specification.
MIL STD	Military Standard.
MOD	Modification.
MOL	Maximum Ordering Limit (Federal Supply Service).
NASA	National Aeronautics and Space Administration.
NIST	National Institute of Standards and Technology.
NCS	National Communications System; responsible for setting U.S. Government standards administered by GSA; also holds primary responsibility for emergency communications planning.
NSA	National Security Agency.
NSEP	National Security and Emergency Preparedness.
NSF	National Science Foundation.
NSIA	National Security Industrial Association.
NTIA	National Telecommunications and Information Administration of the Department of Commerce; replaced the Office of Telecommunications Policy in 1970 as planner and coordinator for government communications programs; primarily responsible for radio.
NTIS	National Technical Information Service.
Obligation	"Earmarking" of specific funding for a contract from committed agency funds.
OFCC	Office of Federal Contract Compliance.
Off-Site	Services to be provided near but not in government facilities.
OFPP	Office of Federal Procurement Policy.
OIRM	Office of Information Resources Management.
O&M	Operations & Maintenance.
OMB	Office of Management and Budget.
O, M&R	Operations, Maintenance, and Readiness.
On-Site	Services to be performed on a government installation or in a specified building.
OPM	Office of Procurement Management (GSA) or Office of Personnel Management.

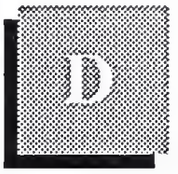
Options	Sole-source additions to the base contract for services or goods to be exercised at the government's discretion.
OSI	Open System Interconnect.
OTA	Office of Technology Assessment (Congress).
Out-Year	Proposed funding for fiscal years beyond the Budget Year (next fiscal year).
P-I	FY Defense Production Budget.
PAR	Procurement Authorization Request or Procurement Action Report.
PCO	Procurement Contracting Officer.
PO	Purchase Order or Program Office.
POM	Program Objective Memorandum.
POSIX	Portable Open System Interconnection Exchange.
POTS	Purchase of Telephone Systems.
PR	Purchase Request or Procurement Requisition.
PRA	Paperwork Reduction Act.
PS	Performance Specification - alternative to a Statement of Work, when work to be performed can be clearly specified.
QMCS	Quality Monitoring and Control System (DoD software).
QMR	Qualitative Material Requirement (Army).
QPL	Qualified Products List.
R-I	FY Defense RDT&E Budget.
RAM	Reliability, Availability, and Maintainability.
RC	Requirements Contract.
R&D	Research and Development.
RDT&E	Research, Development, Test, and Engineering.
RFI	Request For Information.
RFP	Request For Proposal.
RFQ	Request For Quotation.
RFTP	Request For Technical Proposals (Two-Step).
ROC	Required Operational Capability.
SBA	Small Business Administration.
SB Set-Aside	Small Business Set-Aside contract opportunities with bidders limited to certified small businesses.
SCN	Specification Change Notice.
SDN	Secure Data Network.
SE&I	Systems Engineering and Integration.
SETA	Systems Engineering/Technical Assistance.
Sole Source	Contract award without competition.
Solicitation	Invitation to submit a bid.
SOR	Specific Operational Requirement.

SOW	Statement of Work.
SSA	Source Selection Authority (DoD).
SSAC	Source Selection Advisory Council.
SSEB	Source Selection Evaluation Board.
SSO	Source Selection Official (NASA).
STU	Secure Telephone Unit.
Synopsis	Brief Description of contract opportunity in CBD after D&F and before release of solicitation.
TA/AS	Technical Assistance/Analysis Services.
TCP/IP	Transmission Control Protocol/Internet Protocol.
TEMPEST	Studies, inspections, and tests of unintentional electromagnetic radiation from computer, communication, command, and control equipment that may cause unauthorized disclosure of information; usually applied to DoD and security agency testing programs.
TOA	Total Obligational Authority (Defense).
TR	Temporary Regulation (added to FPR, FAR).
TRCO	Technical Representative of the Contracting Offices.
TREAS	Department of Treasury.
TRP	Technical Resources Plan.
TSP	GSA's Teleprocessing Services Program.
TVA	Tennessee Valley Authority.
UCAS	Uniform Cost Accounting System.
USA	U.S. Army.
USAF	U.S. Air Force.
USCG	U.S. Coast Guard.
USMC	U.S. Marine Corps.
USN	U.S. Navy.
U.S.C.	United States Code.
USPS	United States Postal Service.
USRRB	United States Railroad Retirement Board.
VA	Department of Veterans Affairs.
VIABLE	Vertical Installation Automation BaseLine (Army).
VICI	Voice Input Code Identifier.
WIN	WWMCCS Intercomputer Network.
WITS	Washington Interagency Telecommunications System.
WIS	WWMCCS Information Systems.
WS	Work Statement - Offerer's description of the work to be done (proposal or contract).
WWMCCS	World-Wide Military Command and Control System.

B

General and Industry Acronyms

ADAPSO	Association of Data Processing Service Organization, now the Computer Software and Services Industry Association.
ADP	Automatic Data Processing.
ADPE	Automatic Data Processing Equipment.
ANSI	American National Standards Institute.
BOC	Bell Operating Company.
CAD	Computer-Aided Design.
CAM	Computer-Aided Manufacturing.
CBEMA	Computer and Business Equipment Manufacturers Association.
CCIA	Computers and Communications Industry Association.
CCITT	Comite Consultaif Internationale de Telegraphique et Telephonique; Committee of the International Telecommunication Union.
COBOL	COmmon Business-Oriented Language.
COS	Corporation for Open Systems.
CPU	Central Processing Unit.
DBMS	Data Base Management System.
DRAM	Dynamic Random Access Memory.
EIA	Electronic Industries Association.
EPROM	Erasable Programmable Read-Only-Memory.
IEEE	Institute of Electrical and Electronics Engineers.
ISDN	Integrated Services Digital Networks.
ISO	International Organization for Standardization; voluntary international standards organization and member of CCITT.
ITU	International Telecommunication Union.
LSI	Large-Scale Integration.
MFJ	Modified Final Judgement.
PROM	Programmable Read-Only Memory.
RBOC	Regional Bell Operating Company.
UNIX	AT&T Proprietary Operating System.
UPS	Uninterruptable Power Source.
VAR	Value-Added Retailer.
VLSI	Very Large Scale Integration.
WORM	Write-Once-Read-Many-Times.



Appendix: Policies, Regulations, and Standards

A

OMB Circulars

A-11	Preparation and Submission of Budget Estimates.
A-49	Use of Management and Operating Contracts.
A-71	Responsibilities for the Administration and Management of Automatic Data Processing Activities.
A-76	Policies for Acquiring Commercial or Industrial Products and Services Needed by the Government.
A-109	Major Systems Acquisitions.
A-120	Guidelines for the Use of Consulting Services.
A-121	Cost Accounting, Cost Recovery, and Integrated Sharing of DataProcessing Facilities.
A-123	Internal Control Systems.
A-127	Financial Management Systems.
A-130	Management of Federal Information Resources.
A-131	Value Engineering.

B

GSA Publications

The FIRMR as published by GSA is the primary regulation for use by federal agencies in the management, acquisition, and use of both ADP and telecommunications information resources.

C

DoD Directives

DD-5000.1	Major System Acquisitions.
DD-5000.2	Major System Acquisition Process.
DD-5000.11	DoD Data Elements and Data Codes Standardization Program.
DD-5000.31	Interim List of DoD-Approved High-Order Languages.
DD-5000.35	Defense Acquisition Regulatory Systems.
DD-5200.1	DoD Information Security Program.
DD-5200.28	Security Requirements for Automatic Data Processing (ADP) Systems.

	DD-5200.28-M	Manual of Techniques and Procedures for Implement ing, Deactivating, Testing, and Evaluating Secure Resource Sharing ADP Systems.
	DD-7920.1	Life Cycle Management of Automated Information (AIS).
	DD-7920.2	Major Automated Information Systems Approval Process.
	DD-7935	Automated Data Systems (ADS) Documentation.

D

Standards		
	ADCCP	Advanced Data Communications Control Procedures; ANSI Standard X3.66 of 1979; also NBS FIPS 71.
	CCITT G.711	International PCM standard.
	CCITT T.0	International standard for classification of facsimile apparatus for document transmission over telephone-type circuits.
	DEA-1	Proposed ISO standard for data encryption based on the NBS DES.
	EIA RS-170	Monochrome video standard.
	EIA RS-170A	Color video standard.
	EIA RS-464	EIA PBX standards.
	EIA RS-465	Standard for Group III facsimile.
	EIA RS-466	Facsimile standard; procedures for document transmission in the General Switched Telephone Network.
	EIA RS-232-C	EIA DCE to DTE interface standard using a 25-Pin connector; similar to CCITT V-24.
	EIA RS-449	New EIA standard DTE to DCE interface which replaces RS-232-C.
	FED-STD 1000	Proposed Federal Standard for adoption of the full OSI reference model.
	FED-STD 1026	Federal Data Encryption Standard (DES) adopted in 1983; also FIPS 46.
	FED-STD 1041	Equivalent to FIPS 100.
	FED-STD 1061	Group II Facsimile Standard (1981).
	FED-STD 1062	Federal standard for Group III facsimile; equivalent to EIA RS-465.
	FED-STD 1063	Federal facsimile standard; equivalent to EIA RS-466.
	FED- STDs 1005, 1005A-1008	Federal Standards for DCE Coding and Modulation.
	FIPS 46	NBS Data Encryption Standard (DES).
	FIPS 81	DES Modes of Operation.
	FIPS 100	NBS Standard for packet-switched networks; subset of 1980 CCITT X.25.
	FIPS 107	NBS Standard for local-area networks, similar to IEEE 802.2 and 802.3.

FIPS 146	Government Open Systems Interconnection (OSI) Profile (GOSIP).
FIPS 151	NIST POSIX (Portable Operating System Interface for UNIX) standard.
IEEE 802.2	OSI-Compatible IEEE standard for data-link control in local-area networks.
IEEE 802.3	Local-area network standard similar to Ethernet.
IEEE 802.4	OSI-compatible standard for token-bus local area networks.
IEEE 802.5	Local-area networks standard for token-ring networks.
IEEE P1003.1	POSIX standard, similar to FIPS 151.
MIL-STD-188-114C	Physical interface protocol similar to RS-232 and RS-449.
MIL-STD-1777	IP-Internet Protocol.
MIL-STD-1778	TCP - Transmission Control Protocol.
MIL-STD-1780	File Transfer Protocol.
MIL-STD-1781	Simple Mail Transfer Protocol (electronic mail).
MIL-STD-1782	TELNET - virtual terminal protocol.
MIL-STD-1815A	Ada Programming Language Standard.
SVID	UNIX System Interface Definition.
X.12	ANSI standard for Electronic Data Interchange.
X.21	CCITT Standard for interface between DTE and DCE for synchronous operation on public data networks.
X.25	CCITT standard for interface between DTE and DCE for terminals operating in the packet mode on public data networks.
X.75	CCITT standard for links that interface different packet networks.
X.400	ISO Application-level standard for the electronic transfer of messages (electronic mail).

E

Federal Information Processing Standards (FIPS) and Special Publications

FIPS PUB 31	"Guidelines for Automatic Data Processing Physical Security and Risk Management," June 1974.
FIPS PUB 38	"Guidelines for Documentation of Computer Programs and Automated Data Systems," February 15,1976.
FIPS PUB 41	"Computer Security Guidelines for Implementing the Privacy Act of 1974," May 30,1975.
FIPS PUB 64	"Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase," August 1,1979.
FIPS PUB 65	"Guidelines for Automatic Data Processing Risk Analysis," August 1, 1979.
FIPS PUB 73	"Guidelines for Security of Computer Applications," June 30, 1980.
FIPS PUB 101	"Guidelines for Lifecycle Validation, Verification and Testing of Computer Software," June 6, 1983.

FIPS PUB 102	"Guidelines for Computer Security Certification and Accreditation," September 27,1983.
Special Publication 500-105	"Guide to Software Conversion Management," October 1983.
Special Publication 600-148	"Application Software Prototyping and Fourth Generation Languages," May 1987 (and a preceding draft).
Special Publication 500-153	"Auditing and Controls", April 1988.

F

DoD Trusted Computer System Security Level Rankings

Computer security rankings as defined in the Department of Defense (DoD) Trusted Computer System Evaluation Criteria (DoD) 5200.28-STD) are as follows:

Class (D) Minimal protection—This class is reserved for those systems that have been evaluated but fail to meet the requirements for a higher evaluation class.

Class (C1) Discretionary security protection—The Trusted Computer Base (TCB) of a class (C1) system nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis, that is ostensibly suitable for allowing users to be able to protect project or private information and to keep other users form reading or destroying their data accidentally. The class (C1) environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.

Class (C2) Controlled access protection—Systems in this class enforce a more finely grained discretionary access control than (C1) systems, making users individually accountable for their actions through logging procedures, auditing of security related events and resource isolation.

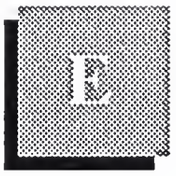
Class (B1) Labeled security protection—Class (B1) systems require all the features required for class (C2). In addition, an informal statement of the security policy model, data labeling and mandatory access control over named subjects and objects must be present. The capability must exist for labeling exported information accurately. Any flaws identified by testing must be removed.

Class (B2) Structured protection—In class (B2) systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class (B1) systems to be extended to all subjects and objects in the ADP system. In addition, covert channels are addressed. The TCB must be structured carefully into protection-critical and nonprotection-critical elements. The TCB interface is well defined, and the TCB design

and implementation enable it to be subjected to more thorough testing and more complete review. Authentication mechanisms are strengthened; trusted facility management is provided in the form of support for system administrator and operator functions; and stringent configuration management controls are imposed. The system is relatively resistant to penetration.

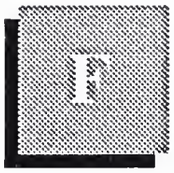
Class (B3) Security domains—The class (B3) TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamperproof and be small enough to be subjected to analysis and tests. To this end, the TCB is structured to exclude code not essential to security policy enforcement, with significant system engineering during TCB design and implementation directed toward minimizing its complexity. A security administrator is supported; audit mechanisms are expanded to signal-relevant events; and system recovery procedures are required. The system is highly resistant to penetration.

Class (A1) Verified design—Systems in class (A1) are functionally equivalent to those in class (B3) in that no additional architectural features or policy requirements are added. The distinguishing feature of systems in this class is the analysis derived from the formal design specification and verification techniques and the resulting high degree of assurance that the TCB is implemented correctly. This assurance is developmental in nature, starting with a formal model of the security policy and a formal top level specification of the design. In keeping with the extensive design and development analysis of the TCB required of systems in class (A1), more stringent configuration management is required, and procedures are established for securely distributing the system to sites. A system security administrator is supported.



Appendix: Related INPUT Reports

A	
Annual Market Analyses	*U.S. Information Services Vertical Markets, 1989*
	U.S. Information Services Cross-Industry Markets, 1988
	Procurement Analysis Reports, GFY 1990-1995
B	
Industry Surveys	*U.S. Information Services Industry, 1989*
	Eighteenth Annual ADAPSO Survey of the Computer Services Industry
	Directory of Leading U.S. Information Services Vendors, 1989
C	
Market Reports	*Federal Large-Scale Systems Market, 1988-1993*
	Federal Professional Services Market, 1989-1994
	Federal Software and Related Services Market, 1989-1994
	Federal Midsize Systems Market, 1988-1993
	Federal Processing Services/Systems Operations Market, 1989-1994
	Federal Systems Integration Market, 1989-1994
	Federal Telecommunications Market, 1988-1993
	Federal Office Information Systems Market, 1988-1993
	Federal Microcomputer Market, 1989-1994
	Defense Logistics Agency Information Services Market
	NASA Information Systems Market, 1988-1993



Appendix: INPUT Questionnaire—Federal Agencies

This questionnaire is directed to the study of the federal market for hardware, software and services to support federal security concerns. It also focuses on the present and future compliance with the Computer Security Act of 1987 and other regulations.

Interviewer: _____

Respondent Name: _____

Title: _____ Phone: _____

Department: _____ Agency: _____

Address: _____

_____

_____

Office Code: _____

Function: _____

Referrals: _____

_____

Confidential

Agency Questionnaire—Federal Computer Security Market

1a. With respect to the Computer Security Act of 1987, what computer security measures have already been adapted by your agency?

- ❑ Identified all systems with sensitive information.
- ❑ Completed security plans for each system.
- ❑ Security implementation.

1b. What measures are planned for the next 2-5 years?

_____

_____

2. In your opinion, what type of computers are most vulnerable to security problems?
Microcomputers ❑ Mainframes ❑ Midsize ❑

Why?_____

_____

3. Since the publicity concerning "Computer Viruses," what steps if any, has your agency taken to protect your computers?

_____

_____

4. What additional directives and guidelines regarding computer security does your agency use in addition to the Computer Security Act?

_____

_____

5a. What responsibilities does your staff have for implementing computer security?

_____

_____

5b. What computer security training requirements has your organization initiated for its employees?

_____

_____

6a. How has the increase in end-user computing impacted your agency's computer security plans and operations?

6b. How has greater employee awareness of computer security contributed to additional agency requirements for training support?

7a. What do you perceive are the major threats to your system(s)?

- ❑ Site access and damage
- ❑ Data access (disclosure of private, classified, or proprietary data)
- ❑ Data manipulation (file alteration)
- ❑ Software or system manipulation (computer viruses)
- ❑ Other (_____)

7b. What are the functional requirements of your agency's/organization's computer security system?

- ❑ Network security
- ❑ End-user computer or computing access
- ❑ Physical security
  - ❑ Computer center
  - ❑ Remote processing site
  - ❑ PCs in LAN or WAN site
- ❑ Data security
- ❑ Other (_____)

8a. What performance criteria has your agency established for computer security products?

8b. How successful have industry products and services been in meeting the current criteria?

9. What might be the impact of the computer security regulations and policies on the following?

a. Open System Architecture

b. GOSIP

c. CALS Initiatives

d. EDI Initiatives

10a. Which of the following computer security products and services does your agency/organization plan to acquire through FY 1993? *(Check all that apply)*

- ❑ Data encryption equipment
- ❑ Software-driven password security
- ❑ Secure networking products
- ❑ Emission control devices
- ❑ Secure workstations
- ❑ Security training tools
- ❑ TEMPEST products
- ❑ Risk management analysis
- ❑ Communications security products
- ❑ Secure UNIX-based products
- ❑ Contractor assistance for preparation of plans
- ❑ Other contractor support
- ❑ Other computer security devices

10b. Have you or do you intend to use a GSA contractor to support your security needs?

Yes ❑ No ❑

If yes, which contractor and in what way?

_____

_____

11. On a scale of 1-5, with 5 being very important and 1 being not important, please rate the following selection criteria for computer security products and services.

Criteria	Rating				
Encryption features	1	2	3	4	5
Vendor's federal experience	1	2	3	4	5
Password systems	1	2	3	4	5
Ease of implementation	1	2	3	4	5
Vendor's support reputation	1	2	3	4	5
Product price	1	2	3	4	5
Secure network capabilities	1	2	3	4	5
Training features	1	2	3	4	5
Other_____	1	2	3	4	5

12a. In your opinion, who are the most important vendors in the federal computer security market? *(Specify vendor names)*

_____, _____,

_____, _____,

_____, _____

12b. How do you see the market developing? (i.e., Civilian vs. defense-oriented companies, etc.)

_____

_____

13. Which methods of acquisition does your agency use for its purchase of computer security products ? *(Please check all that apply and circle method used most often.)*

- ❑ GSA Schedules
- ❑ RFP for requirement contract
- ❑ RFPs for specific purchase
- ❑ Purchase security devices as part of other procurements
- ❑ Other (_____)

14. What type of vendor or organization appears most appropriate for providing computer security products/services for your agency (organization)?

Hardware vendors	❑	Professional services firms	❑
Software vendors	❑	Systems integrators	❑
Aerospace divisions	❑	Not-for-profit firms	❑
Other (_____)	❑		

15. Any suggestions for improvements to security products or services offered by vendors?

_____

_____

16. How would you rate the following computer security vendor characteristics with respect to performance for your agency?
(1=Definitely not satisfactory, 2=Somewhat satisfactory, 3=Satisfactory, 4=Very satisfactory, 5=Outstanding performance)

Characteristic	Rating				
1. Encryption experience	1	2	3	4	5
2. Training experience	1	2	3	4	5
3. Successful implementation	1	2	3	4	5
4. Price	1	2	3	4	5
5. Staff experience	1	2	3	4	5
6. Hardware offered	1	2	3	4	5
7. Software offered	1	2	3	4	5
8. Support experience	1	2	3	4	5
9. Delivery schedule	1	2	3	4	5
10. Other (_____)	1	2	3	4	5

IMPACTS/TRENDS

17. How are technological changes affecting your agency's computer security requirements through FY 1993?

Technology	Impact

18. Could you please identify those industry or market factors (non-technical) that would have the greatest impact on your agency's computer security plans? Include industry mergers, business trends, etc.

19. What impact, if any, have federal government budgetary constraints had on implementing the agency's computer security plans ?

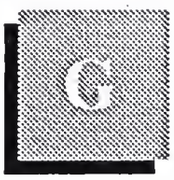
20. How will government policies or regulations from each of the following government agencies impact your agency's/organization's computer security requirements and acquisitions through FY 1993?

a. NIST

b. NSA

c. GSA

Any other policy initiatives by regulatory or legislative organizations?



Appendix: INPUT Questionnaire—Industry Vendors

Interviewer: _____

Respondent Name: _____

Title: _____ Phone: _____

Company: _____

Address: _____

_____

_____

Office Code: _____

Function: _____

Note: Would your company be available to provide a case study example of a recent installation of an agency computer security system?

Yes ❑ No ❑

If so, Agency Program Title: _____

Company Point of Contact:(Name) _____
(Phone)_____

Please return this questionnaire by _____ in the enclosed envelope.

THANK YOU FOR YOUR COOPERATION

Confidential

Industry Questionnaire—Federal Computer Security Market

This questionnaire is directed to the study of the federal market for hardware, software and services to support federal security concerns. It also focuses on the present and future compliance with the Computer Security Act of 1987 and other regulations.

1. Does your company now provide or plan to provide computer security products and related services to the federal marketplace?
   Yes ❑ No ❑ ***(If no, close interview)***

2. Which of the following computer security products and services does your company provide or plan to provide to the federal agencies? ***(Please check all that apply)***
   - ❑ Data encryption equipment
   - ❑ Software-driven password security
   - ❑ Secure networking products
   - ❑ Emission control devices
   - ❑ Secure workstations
   - ❑ Security training tools
   - ❑ TEMPEST products
   - ❑ Risk management analysis
   - ❑ Communications security products
   - ❑ Secure UNIX-based products
   - ❑ Contractor assistance for preparation of plans
   - ❑ Other contractor support
   - ❑ Other computer security devices

3a. What rate of growth do you estimate for the federal computer security market over the next two to five years?
   _____ % estimate

3b. Does your company think its revenues will increase, decrease, or remain constant in this segment of the federal market through FY 1993 and why? ***(Check one and explain)***
   ❑ increasing because:

   _____

   ❑ decreasing because:

   _____

   ❑ remaining the same because:

   _____

4. In your opinion, which federal agencies present the best marketing opportunities for the equipment and services your company provides?
   DoD Including:

   _____

   Civil Agencies Including:

   _____

5. How do the federal defense and civilian markets differ?

   _____

   _____

   _____

6. What methods of government procurement does your company use for federal marketing of computer security products and services?
   - ❑ GSA Schedules
   - ❑ RFPs for specific purchase
   - ❑ Requirement contracts
   - ❑ Install security products as part of other procurements
   - ❑ Other methods (_____)

7. On a scale of 1-5, with 5 being very important and 1 being not important, please rate the following selection criteria for computer security products and services.

Criteria	Rating				
Encryption features	1	2	3	4	5
Vendor's federal experience	1	2	3	4	5
Password systems	1	2	3	4	5
Ease of implementation	1	2	3	4	5
Vendor's support reputation	1	2	3	4	5
Product price	1	2	3	4	5
Secure network capabilities	1	2	3	4	5
Training features	1	2	3	4	5
Other _____	1	2	3	4	5

8. In your opinion, what specific problems or advantages do vendors face in the federal computer security market?
   Problems:

   _____

   _____

   Advantages:

   _____

   _____

9. Below is a short list of possible types of vendors. Please indicate which type of vendor you believe federal agencies will prefer to award their computer security contracts to in order of preference *(rank order)*. Use a 1,2,3,4 order, where 1 means most preferred. *(Indicate rankings below)*

Vendor Rank	Rank
Hardware vendors	_____
Systems integrators	_____
Professional services firms	_____
Software manufacturers	_____
Aerospace divisions	_____
Not-for-profit firms	_____
Other (_____)	_____

10. In your opinion, who are some of the leading vendors in the federal computer security market? *(Specify vendor names)*

    _____

    _____

11a. Based on either your company's current or past contract experience, how would you rate the overall success level of your teaming relationship with other hardware, software, professional services vendors, etc.?

Rate using a 1-5 scale, where 5 means extremely successful, and 1 means not successful at all.
(Circle response) 1 2 3 4 5
No response/no teaming experience ❑

11b. Which types of vendor(s) do you usually team with in your federal computer security contracts?

_____

_____

12. How would you rate the following vendor characteristics with respect to performance by industry vendors to the federal government? ***(1= Definitely not satisfactory, 2=Somewhat satisfactory, 3=Satisfactory, 4=Very satisfactory, 5=Outstanding performance.)***

Characteristic	Rating				
1. Encryption experience	1	2	3	4	5
2. Training experience	1	2	3	4	5
3. Successful implementation	1	2	3	4	5
4. Price	1	2	3	4	5
5. Staff experience	1	2	3	4	5
6. Hardware offered	1	2	3	4	5
7. Software offered	1	2	3	4	5
8. Support experience	1	2	3	4	5
9. Delivery schedule	1	2	3	4	5
10. Other (_____)	1	2	3	4	5

13. What would you like to see vendors do in the next two to five years to make their products and services more valuable to the federal computer security market?

_____

_____

IMPACTS/TRENDS

14. How are technological changes affecting the federal government's security system requirements through FY 1993?

Technology	Impact
_____	_____
_____	_____
_____	_____
_____	_____

15. Please identify those industry or market factors (non-technical) that would have the greatest impact on federal agencies' security system plans? ***(Include industry mergers, business trends, etc.)***

_____

_____

_____

_____

16. What impact, if any, have federal government budgetary constraints had on the agencies' developing and implementing their computer security plans?

_____

_____

17. How will government policies or regulations from each of the following government agencies impact the federal government's computer security requirements and acquisitions through FY 1993?

a. NIST _____

_____

b.NSA _____

_____

c. GSA _____

_____

Any other policy initiatives by regulatory or legislative organizations?

_____

_____

18. What might be the impact of computer security regulations and policies on the following?

a. Open System Architecture

_____

_____

b. GOSIP

_____

_____

c. CALS Initiatives

_____

_____

d. EDI Initiatives

_____

_____

19. What was your company's total corporate revenue for FY 1988? Estimated revenue $_____

20. What percent of your company's revenues is derived from the federal computer security market? _____%

About INPUT

Company Profile

INPUT provides planning information, analysis, and recommendations to managers and executives in the information processing industries. Through market research, technology forecasting, and competitive analysis, INPUT supports client management in making informed decisions.

Continuous-information advisory services, proprietary research/ consulting, merger/acquisition assistance, and multiclient studies are provided to users and vendors of information systems and sevices (software, processing services, turnkey systems, systems integration, professional services, communications, and systems/software maintenance and support).

Many of INPUT's professional staff have more than 20 years experience in their areas of specialization. Most have held management positions in large organizations, enabling them to supply practical solutions to complex business problems.

Formed as a privately held corporation in 1974, INPUT has become a leading international research and consulting firm. Clients include more than 100 of the world's largest and most technically advanced companies.

Staff Credentials

INPUT's staff have been selected for their broad background in a variety of functions, including planning, marketing, operations, and information processing. Many of INPUT's professional staff have held executive positions in some of the world's leading organizations, both as vendors and users of information services, in areas such as the following:

- Processing Services
- Professional Services
- Turnkey Systems
- Applications Software
- Field (customer) Service
- Banking and Finance
- Insurance
- Process Manufacturing
- Telecommunications
- Federal Government

Educational backgrounds include both technical and business specializations, and many INPUT staff hold advanced degrees.

U.S. and European Advisory Services

INPUT offers the following advisory services on an annual subscription basis.

1. Market Analysis Program—U.S.
The Market Analysis Program provides up-to-date U.S. information services market analyses, five-year forecasts, trend analyses, vertical/cross-industry market reports, an on-site presentation, hotline inquiry service, and sound recommendations for action. It covers software, professional and network services, turnkey systems, and professional services markets. It is designed to satisfy the planning and marketing requirements of current and potential information services vendors.

2. Market Analysis Program—Europe
This program is designed to help vendors of software and services with their market planning. It examines the issues in the marketplace, from both a user and a vendor viewpoint. It provides detailed five-year market forecasts to help plan for future growth.

3. Vendor Analysis Program—U.S.
A comprehensive reference service covering more than 400 U.S. information services vendor organizations, VAP is often used for competitive analysis and prescreening of acquisition and joint-venture candidates. Profiles on leading vendors are updated regularly, and hotline inquiry service is provided.

4. Vendor Analysis Program—Europe
This is an invaluable service for gaining competitve information. Two binders are provided—one is a directory listing names, addresses, and turnover of some 700 European software and services vendors. The second binder contains profiles of about 300 key vendors.

5. Electronic Data Interchange Program—U.S.
Focusing on what is fast becoming a major computer/communications market opportunity, this program keeps you well informed. Through monthly newsletters, timely news flashes, comprehensive studies, a joint user/vendor conference, and telephone inquiry privileges, you will be informed and stay informed about the events and issues impacting this burgeoning market.

6. Network Services Program—Europe
Network services is a fast-growing area of the software and services industry. This program is essential to vendors of EDI, electronic information services, and network products and services. It keeps clients informed of the latest developments and includes a monthly newsletter on EDI.

7. Systems Integration Program—U.S.
Focus is on the fast-moving world of systems integration and the provision of complex information systems requiring vendor management and installation of multiple products and services. The program includes an annual market analysis of the U.S. systems integration and operations markets, SI vendor profiles and updates, topical market analysis reports, and an annual SI seminar.

8. Systems Operations Program—U.S.
This program includes an annual market analysis report of the systems operations and systems integration market, SO vendor profiles and updates, reports on network management and SO management practices, and an annual SO seminar.

9. Systems Management Program—Europe
Systems integration and systems operations (facilities management) are key growth areas for the decade. This program examines these two areas and analyzes current market trends, user needs, and vendor offerings.

10. Federal Information Systems and Services Program
This program presents highly specific information on U.S. federal government procurement practices, identifies information services vendor opportunities, and provides guidance from INPUT's experienced Washington professionals to help clients maximize sales effectiveness in the federal government marketplace.

11. Information Systems Program
ISP is designed for executives of large information systems organizations and provides crucial information for planning, procurement, and management decision making. This program is widely used by both user and vendor organizations.

12. Customer Service Program—International
This program provides customer service organization management with data and analyses needed for marketing, technical, financial, and organizational planning. The program pinpoints user perceptions of service received, presents vendor-by-vendor service comparisons, and analyzes and forecasts service markets for large systems, minicomputers, personal computer systems, and third-party maintenance. A monthly newsletter helps clients keep informed of the latest developments in the market.

13. Customer Service Program—Europe
Customer service is an expanding area. Companies are now expanding from hardware service to more software-related maintenance and professional services. This program helps vendors penetrate these new areas and provides guidelines for future market strategy. A monthly newsletter helps clients keep abreast of the latest developments in the market.

14. Worldwide Information Services Market Forecasts, 1989-1994
In 1989 INPUT initiated this research study, which provides an international forecast for the information services market.

15. INPUT's sales office in Japan
Provides research services on U.S. and global information services to Japanese clients.

Customized Advisory Services

In addition to standard continuous-information programs, INPUT will work with you to develop and provide a customized advisory service that meets your unique requirements.

Acquisition Services

INPUT also offers acquisition services that are tailor-made for your requirements. INPUT's years of experience and data base of company information about information systems and services companies have helped many companies in their acquisition processes.

An Effective Combination

INPUT'S Executive Advisory Services are built on an effective combination of research-based studies, client meetings, informative conferences, and continuous client support. Each service is designed to deliver the information you need in the form most useful to you, the client. Executive Advisory Services are composed of *varied combinations of the following products and services:*

Research-Based Studies
Following a proven research methodology, INPUT conducts major research studies throughout each program year. Each year INPUT selects issues of concern to management. Topical reports are prepared and delivered throughout the calendar year.

Information Service Industry Reports
INPUT's Executive Advisory Services address specific issues, competitive environments, and user expenditures relative to:

- Software
- Processing/Network Services
- Systems Integration
- Telecommunications Service
- Office Systems
- Professional Services
- Turnkey Systems
- Small-Systems Service
- Third-Party Maintenance
- Large-Systems Service

Industry-Specific Market Reports

Detailed analyses of market trends, forces driving the markets, problems, opportunities, and user expenditures are available for the following sectors:

- Discrete Manufacturing
- Process Manufacturing
- Transportation
- Utilities
- Telecommunications
- Retail Distribution
- Wholesale Distribution
- Banking and Finance
- Insurance
- Medical
- Education
- Business and Technical Services
- Consumer Services
- Federal Government
- State and Local Government
- Other Industry Sectors

Cross-Industry Market Report

A separate analysis covers the following cross-industry application areas:

- Accounting
- Education and Training
- Engineering and Scientific
- Human Resources
- Office Systems
- Planning and Analysis
- Other Cross-Industry Sectors

Hotline: Client Inquiry Services

Inquiries are answered quickly and completely through use of INPUT's Client Hotline. Clients may call any INPUT office (California, New York, Washington D.C., London, or Paris) during business hours or they may call a unique voicemail service to place questions after hours. This effective Hotline service is the cornerstone of every INPUT Executive Advisory Service.

The Information Center

One of the largest and most complete collections of information services industry data, the Information Center houses literally thousands of up-to-date files on vendors, industry markets, applications, current/emerging technologies, and more. Clients have complete access to the Information Center. In addition to the information contained in its files, the center maintains an 18-month inventory of over 130 major trade publications, vendor consultant manuals, economic data, government publications, and a variety of important industry documents.

Access to INPUT Professional Staff

Direct access to INPUT's staff, many of whom have more than 20 years of experience in the information industry, provides you with continuous research and planning support. When you buy INPUT, you buy experience and knowledge.

Annual Client Conference
Each year, you can attend INPUT's Annual Client Conference. This event addresses the status and future of the information services industry, the competitive environment, important industry trends potentially affecting your business, the impact of new technology and new service offerings, and more.

You will attend with top executives from many of the industry's leading, fastest-growing, and most successful vendor companies—and with top Information Systems (IS) managers from some of the world's most sophisticated user organizations.

On-Site Presentation by INPUT Executives
Many of INPUT's programs offer an informative presentation at your site. Covering the year's research, this session is held in the fourth quarter of each calendar year.

Proprietary Research Service

INPUT conducts proprietary research that meets the unique requirements of an individual client. INPUT's custom research is effectively used:

For Business Planning
Planning for new products, planning for business startups, planning for expansion of an existing business or product line—each plan requires reliable information and analysis to support major decisions. INPUT's dedicated efforts and custom research expertise in business planning ensure comprehensive identification and analysis of the many factors affecting the final decision.

For Acquisition Planning
Successful acquisition and divestiture of information services companies requires reliable information. Through constant contact with information services vendor organizations and continuous tracking of company size, growth, financials, and management "chemistry," INPUT can provide the valuable insight and analysis you need to select the most suitable candidates.

For the Total Acquisition Process
INPUT has the credentials, the data base of company information, and—most importantly—the contacts to assist you with the total acquisition and/or partnering relationship processes:

- Due Diligence
- Schedules and Introduction
- Criteria & Definitions
- Retainer and Fee-Based
- Active Search

For Competitive Analysis

Knowing marketing and sales tactics, product capabilities, strategic objectives, competitive postures, and strengths and weaknesses of your competition is as critical as knowing your own. The career experience of INPUT's professionals—coupled with INPUT's collection and maintenance of current financial, strategic, tactical, and operational information about more than 400 active companies—uniquely qualifies INPUT to provide the best competitive information available today.

For Market and Product Analysis

Developing new products and entering new markets involves considerable investment and risk. INPUT regularly conducts research for clients to identify product requirements, market dynamics, and market growth.

More About INPUT...

- More than 5,000 organizations, worldwide, have charted business directions based on INPUT's research and analysis.
- Many clients invest more than $50,000 each year to receive INPUT's recommendations and planning information.
- INPUT regularly conducts proprietary research for some of the largest companies in the world.
- INPUT has developed and maintains one of the most complete information industry libraries in the world (access is granted to all INPUT clients).
- INPUT clients control an estimated 70% of the total information industry market.
- INPUT analyses and forecasts are founded upon years of practical experience, knowledge of historical industry performance, continuous tracking of day-to-day industry events, knowledge of user and vendor plans, and business savvy.
- INPUT analysts accurately predicted the growth of the information services market—at a time when most research organizations deemed it a transient market. INPUT predicted the growth of the microcomputer market in 1980 and accurately forecasted its slowdown in 1984.

For More Information . . .

INPUT offers products and services that can improve productivity, and ultimately profit, in your firm. Please give us a call today. Our representatives will be happy to send you further information on INPUT services or to arrange a formal presentation at your offices.

For details on delivery schedules, client service entitlement, or Hotline support, simply call your nearest INPUT office. Our customer support group will be available to answer your questions.

- **California** .....(415) 961-3300
- **New York** .....(201) 299-6999
- **Washington, D.C.** .....(703) 847-6870
- **London** .....(071) 493-9335
- **Paris**.....(33-1) 42-77-42-77
- **Tokyo**.....(03) 864-0531